VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
DEPARTMENT OF INFORMATICS

ZÁLOHOVÁNÍ DAT A DATOVÁ ÚLOŽIŠTĚ

DATA BACKUP AND DATA STORAGES

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — Lukáš Višňovec
AUTHOR

VEDOUCÍ PRÁCE — Ing. Jiří Kříž, Ph.D.
SUPERVISOR

BRNO 2021

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání bakalářské práce

Ústav:	Ústav informatiky
Student:	**Lukáš Višňovec**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Manažerská informatika
Vedoucí práce:	**Ing. Jiří Kříž, Ph.D.**
Akademický rok:	2020/21

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává bakalářskou práci s názvem:

Zálohování dat a datová úložiště

Charakteristika problematiky úkolu:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Cílem práce je návrh řešení pro bezpečné a dlouhodobé ukládání dat různé priority. Podstatou řešení je vytvoření datového toku z privátního externího cloudového úložiště do zabezpečeného interního a redundantního úložiště.

Základní literární prameny:

CUBR, Ladislav. Dlouhodobá ochrana digitálních dokumentů. Praha: Národní knihovna České republiky, 2010. ISBN 978-80-7050-588-5.

JIANG, H. a kol. A secure and scalable storage system for aggregate data in IoT, Futur. Gener. Comput. Syst. 49 (2015) s.133–141.

KUROSE, James F. a Keith W. ROSS. Počítačové sítě. Brno: Computer Press, 2014. ISBN 9788025138250.

POŽÁR, Josef. Manažerská informatika. Plzeň: Aleš Čeněk, 2010. ISBN 978-80-7380-276-9.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2020/21

V Brně dne 28.2.2021

L. S.

Mgr. Veronika Novotná, Ph.D. ředitel	doc. Ing. Vojtěch Bartoš, Ph.D. děkan

Abstrakt

V bakalárskej práci je riešená problematika zálohovania dát a ich ochrany. Dáta spoločnosti podnikajúcej v oblasti IoT, ktorá disponuje dátami získanými od svojich zákazníkov a vlastnými projektovými dátami alebo inými dokumentami. V doterajšom riešení spoločnosť využívala cloudové úložisko. Z dôvodu bezpečnosti a rastúcich požiadaviek na kapacitu úložiska sa v práci rieši návrh bezpečného lokálneho úložiska pre IoT dáta a ostatné archívne dáta. Navrhuje sa koncept dátového centra zo serverovými úložiskami, pričom sa úložisko rozdeľuje na dva celky, prvým väčším celkom je úložisko IoT dát a druhým menším celkom je archivačný server. V návrhu sú ďalej zohľadnené požiadavky na výkon, bezpečnosť a cenu. Postupný presun väčšej časti dát z cloudu do lokálneho úložiska je pre optimalizáciu návrhu riešený blokovo. V prvom bloku sa uvažujú potrebné zmeny na cloude a jeho ďalšie využitie. Druhým blokom je návrh bezpečnej a redundantnej sieťovej infraštruktúry. Tretí blok je tvorený návrhom vlastného úložiska a spôsobu jeho zálohovania s využitím redundantných polí nezávislých diskov.

Kľúčové slová

lokálne dátové úložisko, cloud, zálohovanie dát, RAID, sieťová infraštruktúra, ochrana dát

Abstract

This thesis focuses on the issues of data backup and protection. This data belongs to a company whose business is in the area of IoT. The company obtains the data from their customers, their own project or other documents. Until now the company has used cloud storage. Because of safety and growing requirements for the storage capacity this thesis deals with the design of safe local data storage for IoT and other archive data. A concept of data center with server storage is being proposed while the storage is divided in two parts. The first and bigger part is an IoT data storage and the second and smaller part focuses on archive server. The performance, safety and price requirements are also taken into account. Majority of the data is designed to be gradually trasfered from cloud to local storage by blocks. In the first block the changes needed and the following use of the cloud are being considered. The second block is the design of a safe and redundant network infrastructure. The third block is formed by the design of an own storage and the way of its backup with the use of redundant array of independent disks.

Keywords

local data storage, cloud, data backup, RAID, network infrastructure, data protection

Bibliografická citácia

VIŠŇOVEC, Lukáš. *Zálohování dat a datová úložiště.* Brno, 2021. Dostupné také z: https://www.vutbr.cz/studenti/zav-prace/detail/135483. Bakalářská práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Jiří Kříž.

Čestné prehlásenie

Prehlasujem, že som bakalársku prácu vypracoval samostatne a že všetky použité literárne zdroje som správne a úplne citoval. Bakalárska práca je z hľadiska obsahu majetkom Fakulty podnikateľskej VUT v Brne a môže byť využitá ku komerčným účelom len so súhlasom vedúceho bakalárskej práce a dekana FP VUT.

V Brně, dne 16. 5. 2021 ……

podpis autora

Poďakovanie

Ďakujem môjmu školiteľovi Ing. Jiřímu Křížovi, Ph.D. za ochotu, užitočné rady a konzultácie pri písaní práce. Osobitne ďakujem za pomoc s technickou stránkou návrhu siete Ing. Jozefovi Mindovi. Veľká vďaka patrí taktiež rodine a priateľom, ktorí mi pri mojej práci pomáhali.

Obsah

ÚVOD

Objemy dát a veľkosť dátových tokov, s ktorými aktuálne spoločnosti operujú sú enormné. V súčasnosti do firemných procesov vo veľkej miere vstupuje automatizácia s použitím výpočtovej techniky. S tým súvisí generovanie obrovského množstva dát. Na efektívne využitie veľkých objemov dát je potrebné ich spracovanie a následná analýza. Takto sa z dát získavajú užitočné informácie, ktoré umožňujú výrazné zlepšenie zavedených firemných procesov. Zjednodušene možno povedať, že generovanie procesných dát zo senzorov, aktuátorov a pod. s ich distribúciou pomocou sieťovej infraštruktúry a ich následná analýza je základom moderného konceptu „internetu vecí“ IoT. V tomto koncepte nie sú dôležité len aktuálne dáta, ale aj dáta historické, ktoré slúžia na porovnávanie, zisťovanie zmien alebo sú nejakým spôsobom dôležité. Zároveň platí, že tieto dáta môžu mať pre spoločnosť vysokú cenu a sú zaujímavým cieľom pre potenciálnych útočníkov, ktorí by ich mohli neoprávnene využiť alebo zneužiť. Vyvstáva tak potreba nájsť spôsob na bezpečné uloženie obrovských objemov dát.

Z dôvodu zníženia rizika straty cenných dát spoločnosti, dáta zálohujú. Pri ukladaní a rovnako aj zálohovaní sa berie do úvahy aj bezpečnostné hľadisko ochrany dát. Nejde len o ochranu pred stratou, ale aj odcudzením a ich zneužitím. Tieto požiadavky vyžadujú komplexné riešenie od úrovne zabezpečenia sieťovej infraštruktúry, dátového úložiska až po úroveň ľudského faktoru a nastavenia vhodnej bezpečnostnej politiky pre všetkých, ktorí s dátami prichádzajú do kontaktu. Na trhu je k dispozícii veľké množstvo hardvérových a softvérových nástrojov, ktoré umožňujú firmám zavádzať dátové centrá požadovanej kapacity. Okrem spomínaných bezpečnostných hľadísk sa zvažuje aj efektivita konkrétneho riešenia z pohľadu výkonu a ceny. Vytvoriť efektívne dátové úložisko nie je jednoduchý problém, pretože sa zohľadňuje veľké množstvo vstupných faktorov.

Problematika zálohovania dát v modelovej spoločnosti Prinet, s.r.o., ktorá sa zaoberá analýzou procesných IoT dát od svojich zákazníkov a tieto dáta potrebuje bezpečne uložiť, je riešená v rámci predkladanej práce. Návrh zálohovania dát v lokálnom dátovom úložisku je rozdelený do troch prepojených, ale nezávislých blokov. Vychádza sa z doterajšieho cloudového úložiska, ktoré tvorí prvý blok riešenia s potrebou implementácie niektorých zmien pri snahe previesť zálohovanie z objednaného cloudového priestoru do lokálneho úložiska. Druhým veľkým blokom je sieťová infraštruktúra, ktorá má byť navrhnutá tak, aby bola bezpečná a dostatočne výkonná aj pre umiestnenie úložiska. Posledným tretím blokom návrhu je vlastné úložisko, ktoré je riešené redundantne s využitím diskových polí a dimenzované pre dostatočnú výkonnosť a kapacitu.

CIELE PRÁCE A METÓDY

Hlavným cieľom práce je návrh riešenia pro bezpečné a dlhodobé ukladanie dát rôznej priority. Podstatou riešenia je vytvorenie dátového toku z privátneho externého cloudového úložiska do zabezpečeného interného a redundantného úložiska.

Súčasťou návrhu je nájdenie optimálneho riešenia pre bezpečné a dlhodobé ukladanie dát rôznej priority pre spoločnosť, ktorá sa zaoberá analýzou dát zákazníkov získaných zo senzorov pre zlepšenie nastavenia ich procesov. Podstatou riešenia je vytvorenie dátového toku z privátneho externého cloudového úložiska do interného zabezpečeného a redundantného úložiska. Riešenie zahŕňa algoritmus na prioritizáciu dát, návrh bezpečného toku dát z externého do interného úložiska, zabezpečenie dostatočného zálohovania podľa priority a komplexnú hardvérovú schému. Súčasťou riešenia je návrh optimálnej štruktúry zálohovania, voľba optimálneho nastavenia a ekonomické zhodnotenie.

1 TEORETICKÉ VÝCHODISKÁ PRÁCE

1.1 Zálohovanie a archivácia dát

Zálohovanie dát

Proces duplikovania dát pre možnosť ich obnovy v prípade straty. Zálohovanie dát je kľúčové pre ich úspešnú obnovu [1].

Archivácia dát

Proces, pri ktorom sú neaktívne dáta presunuté zo systému do dlhodobého úložiska. Sú odkladané pre ich prístupnosť v prípade potreby využitia dát. Sú to teda dáta, ktoré sú pre spoločnosť naďalej potrebné, alebo musia byť ukladané z dôvodu regulácií. Archívy sú indexované s možnosťou vyhľadávania pre ich lokalizáciu a následné získanie [2].

Zálohovanie a archivácia dát sú rozdielne pojmy. Zálohovanie je duplikovanie dát, ku ktorému pri archivácii nedochádza. Aj napriek tomu, že sú obidve považované za sekundárne úložisko a využívajú kapacitne väčšie úložné zariadenia ako primárne úložisko, tak majú iné využitie. Archivácia je využívaná na uchovávanie údajov, kde existuje možnosť ich neskoršieho využitia. Záloha primárnych dát naopak slúži na ich ochranu pre prípad potrebnej obnovy [2].

1.1.1 Príčiny straty dát

Strata dát môže mať rôzne príčiny a každá z nich predstavuje iný problém pre potenciálny spôsob obnovy dát. Najčastejšou príčinou je zlyhanie HDD, ľudskou chybou alebo softvérový problém. Povedomie o príčinách straty dát a rizík s nimi spojených je kľúčové pre ochranu pred ich stratou [3].

Ľudská chyba – je spôsobená úmyselným alebo neúmyselným vymazaním, resp. prepisom pôvodných dát novými dátami. Problémom sa dá predchádzať dostatočným zaškolením zamestnancov. Ľudská chyba môže viesť aj k fyzickému ohrozeniu hardvéru, napr. poliatie zariadenia tekutinou, pád a pod. [3].

Vírusy a malware – predstavujú hrozbu ukradnutia, zmazania alebo poškodenia dát čím môžu ohroziť funkčnosť spoločnosti. Ako ochrana slúži antivírus a častá záloha dát [3].

Poškodenie HDD – HDD sú veľmi citlivé a tak sa pri prenášaní môžu jednoducho poškodiť, keďže obsahujú pohyblivé časti. K znefunkčneniu môže viesť zanesenie prachom alebo opotrebenie pohyblivých súčastí. Ďalšie príčiny poškodenia HDD sú: výpadok elektrického prúdu alebo elektrický skrat [3].

Softvérový problém – následkom neočakávaných zlyhaní softvéru sa môžu dáta poškodiť alebo sa neuložia zmeny v dátach vykonané. Ak dôjde ku poškodeniu softvéru znamená to, že dáta v ňom uložené nebudú naďalej prístupné. Preto je potrebné implementovať procedúry, ktoré zaistia bezpečné vypnutie softvéru po každom použití a často aj pri zlyhaní [3].

1.1.2 Typy záloh

Plná záloha – dochádza ku vytváraniu aspoň jednej kópie všetkých dát, ktoré je potrebné zálohovať. Ide o najspoľahlivejší typ zálohy, ale jej prevádzkovanie je časovo a kapacitne náročné. Pri plnej zálohe dochádza ku zálohovaniu všetkých dát súčasne, čím je zjednodušené kontrolovanie verzií. Výhodou je aj vyhľadávanie dát, nakoľko sú všetky dáta na jednom úložisku. Obnova dát je rýchlejšia, pretože sú všetky dáta ihneď dostupné. Nevýhodou je nutnosť väčšej kapacity na zálohu dát. Pri poškodení zálohovacieho úložiska dochádza ku strate celej zálohy [1].

Inkrementálna záloha – typ zálohy, ktorá kopíruje iba tie dáta, ktoré boli zmenené alebo vytvorené od poslednej zálohy. Využíva sa v prípade, že je množstvo dát na každodennú plnú zálohu príliš objemné. Inkrementálna záloha šetrí čas obnovy a miesto na disku. Táto záloha je typickou metódou pre zálohovanie na cloude a to z dôvodu menšej náročnosti na využitie zdrojov [1].

Diferenciálna záloha – je záloha dát, ktorá kopíruje všetky súbory, ktoré boli zmenené od poslednej plnej zálohy. Tá taktiež zahŕňa súbory vytvorené, upravené alebo pozmenené a nekopíruje zakaždým všetky dáta. Celý proces začína vytvorením úplnej zálohy. Od inkrementálnej zálohy sa líši tým, že dáta, ktoré sú pri zálohe kopírované sa porovnávajú s poslednou plnou zálohou [1].

Obrátená inkrementálna záloha – tento typ zálohy je zameraný na zmeny vytvorené medzi dvoma zrkadleniami. Po vytvorení plnej zálohy sa následne každá ďalšia inkrementálna záloha aplikuje tak, aby sa prejavili zmeny v existujúcej plnej zálohe [1].

1.2 Operácie s dátami

Na zálohovanie dát je kľúčovou operáciou najmä ich duplikácia, ktorá sama osebe k zálohe postačuje, avšak pre zvýšenie efektívneho využívania zdrojov sa zavádza proces komprimácie a k zaisteniu bezpečnosti pri prenose a uložení dát sa využíva šifrovanie.

1.2.1 Komprimácia

Táto operácia má v procese zálohovania dát významné využitie pre zníženie výsledného objemu zálohovaných dát, pričom v ideálnom prípade je to bez straty dát alebo stratami dôjde len k minimálnym stratám v dátach. Ide o redukciu počtu bitov potrebných na zobrazenie dát. Komprimácia dát dokáže ušetriť úložnú kapacitu, zrýchliť prenos a znížiť náklady na úložný hardvér a sieťovú šírku pásma. Proces komprimácie je vykonávaný programom, ktorý využíva vzorec alebo algoritmus na rozhodnutie, ako zmenšiť veľkosť dát. Pri komprimácii textu môže dôjsť k vymazaniu nepotrebných znakov. Algoritmus môže zmenšovať reťazce bitov na základe slovníkov pre konverziu medzi reťazcami [4].

1.2.2 Duplikácia

Proces vytvárania presnej kópie dát na iné úložisko. V prípade, že je duplikácia dát vytváraná na ich ochranu pred stratou alebo poškodením, tvoríme zálohu [5].

1.2.3 Šifrovanie

Metóda, pri ktorej sú dáta konvertované do kódu tak, aby neboli zrozumiteľné. Vzorce využívané na šifrovanie a dešifrovanie správ, sú nazývané šifrovacie algoritmy. Šifrovanie je dôležité pre ochranu dát. Šifrovanie je použiteľné aj na ochranu zálohovaných dát, kedy je záloha zakódovaná a aj po jej odcudzení je pre útočníka veľmi ťažké získať pôvodné dáta. Šifrovanie poskytuje [6]:

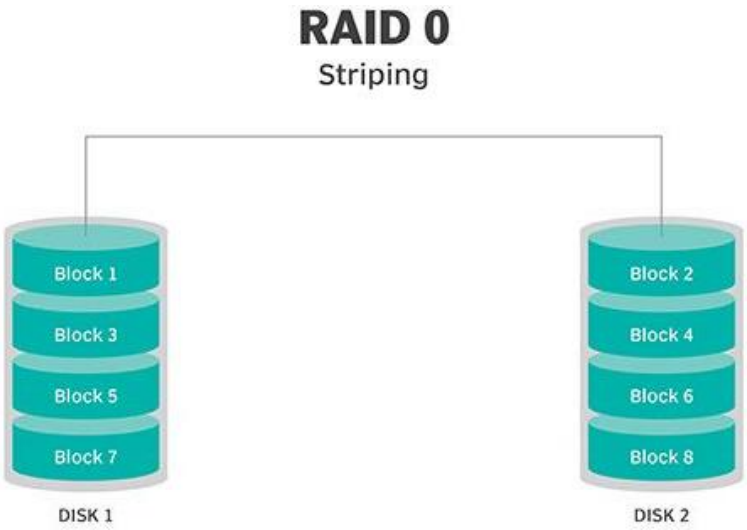
- Dôvernosť – dešifruje obsah správy.
- Overenie – kontroluje pôvod správy.
- Úplnosť – dokazuje, že správy neboli od ich odoslania pozmenené.
- Nepopierateľnosť – zabraňuje odosielateľovi poprieť odoslanie šifrovanej správy.

1.3 Metóda diskových polí RAID

Redundantné pole nezávislých diskov je spôsob zálohy rovnakých dát v rôznych miestach na viacerých HDD alebo SSD pre ochranu dát v prípade zlyhania disku. Funkciu RAID zabezpečuje ovládač, zariadenie, ktoré spravuje HDD v diskovom poli. Využívanie RAID ovládača zvyšuje výkon a pomáha chrániť dáta v prípade zlyhania. RAID sa delí na úrovne a úloha všetkých nie je redundancia [7].

1.3.1 RAID 0

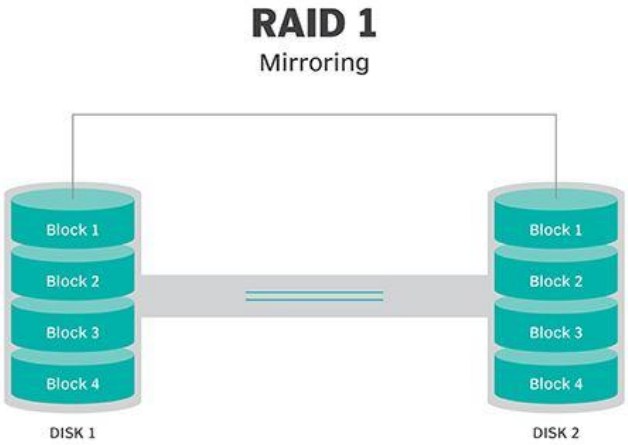
Ide o proces, pri ktorom sú dáta rozdeľované do blokov a následne sú v týchto blokoch súmerne ukladané medzi viacero úložných zariadení, ako sú HDD alebo SSD, ktoré sú zapojené v tomto RAID poli. Metóda je využívaná najmä pre zvýšenie výkonu, keďže sú dáta zapisované na väčší počet diskov, čoho výsledkom je rýchlejší zápis a aj čítanie dát, výsledná rýchlosť je súčtom rýchlosti zápisu na jednotlivé disky. Nedochádza ku redundancii dát, čo je nevýhoda pri zlyhaní niektorého z diskov, pretože dáta z defektného disku nedokážeme získať. RAID 0 je preto využívaný najmä z dôvodu rýchlosti ukladania a čítania. Ide o dáta nepodstatné alebo dáta, ktoré máme uložené aj na inom mieste. Výhodou je pomer ceny a rýchlosti, no naopak nevýhodou je spomínaná možná strata dát. Kapacita je daná veľkosťou najmenšieho disku. Bloková schéma dvoch zrkadlených diskov pri RAID 0 je na Obr. 1.1 [7].



Obr. 1.1: Schéma úložiska typu RAID 0; striping – rozdeľovanie, block - blok [7]

1.3.2 RAID 1

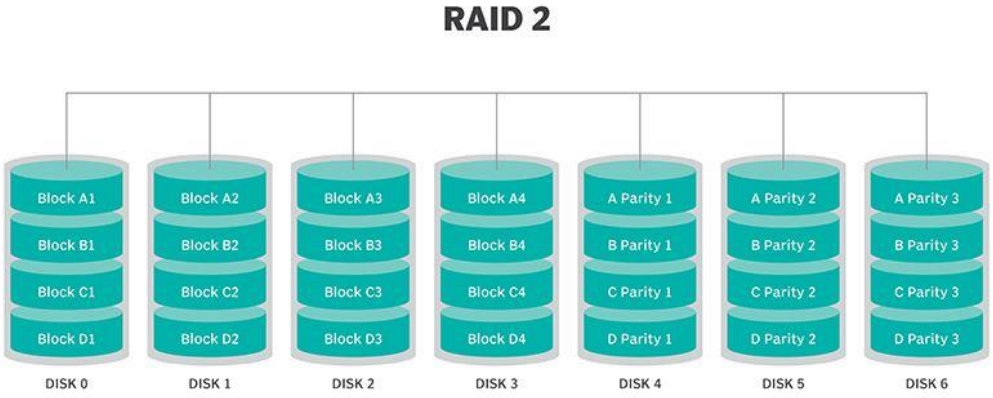
Systém ukladania dát do poľa RAID 1 je známy ako zrkadlenie dát. Ide o identickú replikáciu dát na dva alebo väčší počet diskov. Jeho aplikovanie je vhodné, pokiaľ je dôraz kladený na výkon a dostupnosť. Na všetkých diskoch sú uložené rovnaké dáta, preto môže byť čítanie z nich pomerne rýchle. Toto pole RAID je funkčné aj v prípade, že funguje iba jeden z diskov. Zapisovanie je zase naopak pomalšie a to z dôvodu, že rovnaké dáta zapisujeme viackrát, čo závisí na počte diskov v poli. V prípade zlyhania niektorých diskov sú dáta okamžite čítané zo zvyšných funkčných diskov a tak je vhodný v kritických situáciách. Túto metódu teda využívame najmä, keď je pre nás redundancia prvoradá. Rovnako ako pri RAID 0 je kapacita daná veľkosťou najmenšieho z diskov. Schéma zrkadlenia RAID 1 je na Obr. 1.2 [7].



Obr. 1.2: Schéma úložiska typu RAID 1; mirroring – zrkadlenie, block – blok [7]

1.3.3 RAID 2

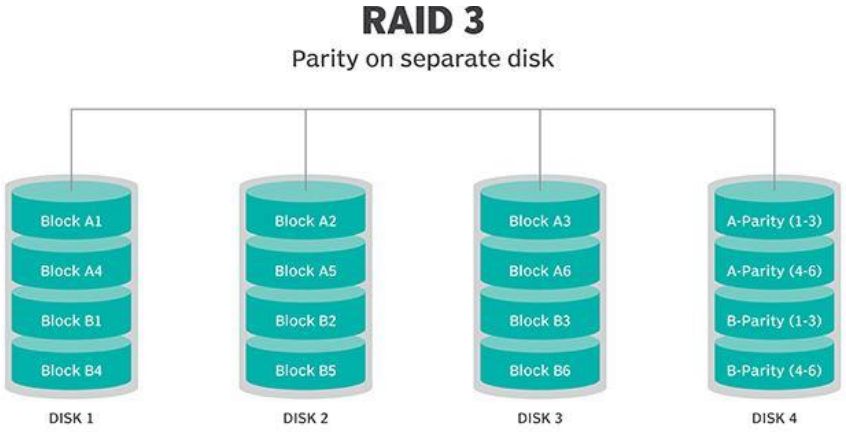
Diskové pole typu RAID 2 už nie je využívané, nakoľko je zastarané. Dáta sú rozdeľované na bitovej úrovni a rotácia diskov je synchronizovaná. V prípade poškodenia niektorého z diskov, je pri oprave chýb využívaný Hammingov kód, ktorý poskytuje paritu. Dnešné HDD tento kód na opravu chýb využívajú a tak sa táto metóda zálohovania naďalej nepoužíva. Výhodou RAID 2 je dobrá ochrana dát, ale vyššia komplexnosť systému zálohovania spôsobuje rast ceny tohto riešenia. Schéma úložiska RAID 2 je na Obr. 1.3 [7].



Obr. 1.3: Schéma úložiska typu RAID 2; parity - parita, block – blok [7]

1.3.4 RAID 3

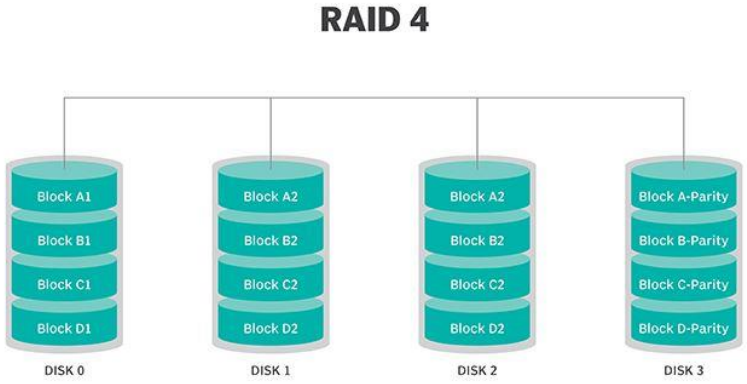
Táto RAID konfigurácia, znázornená na Obr. 1.4, využíva paritný disk na ukladanie informácii generovaných RAID ovládačom namiesto toho, aby boli tieto informácie ukladané spolu s dátami. Z tohto dôvodu nie je dosahovaný vysoký výkon, pri zadávaní mnohých menších požiadaviek, ktoré sú časté napr. v databázach. Naopak poskytuje veľkú priepustnosť, čo je výhodou pri veľkých objemoch dát. Pri tomto RAID sú požadované minimálne 3 fyzické disky a taktiež ako pri RAID 2 je ich rotácia synchronizovaná [7].



Obr. 1.4: Schéma úložiska typu RAID 3; parity on separate disk – parita na oddelenom disku, block – blok, parity – parita [7]

1.3.5 RAID 4

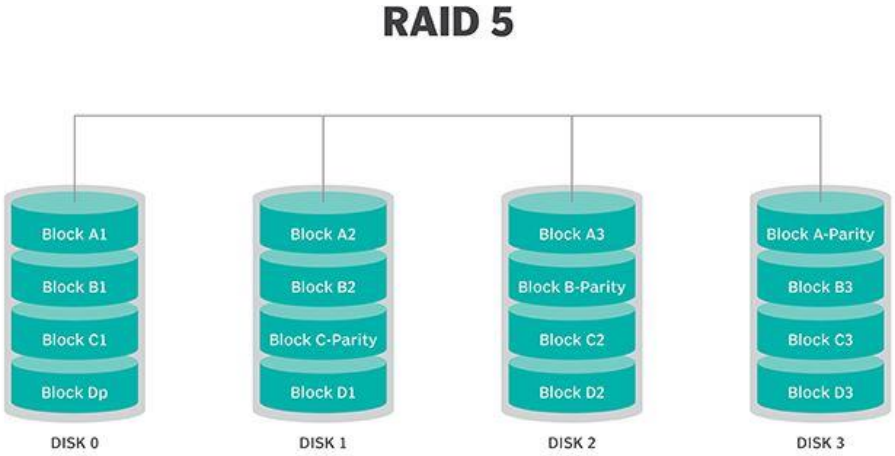
Tento RAID využíva delenie dát na blokovej úrovni na rozdiel od bajtovej, ako tomu je pri RAID 3. Analogicky sa využíva priradený paritný disk, čím sa zabezpečuje ochrana dát. Blokové delenie dát umožňuje prístup k nim z ktoréhokoľvek disku. Výhodou je teda postupný prístup k dátam. Nevýhodou je spomaľovanie všetkých zápisov, z dôvodu simultánneho ukladania informácií na paritný disk. Schéma úložiska RAID 4 je znázornená na Obr. 1.5 [7].



Obr. 1.5: Schéma úložiska typu RAID 4; parity - parita, block – blok [7]

1.3.6 RAID 5

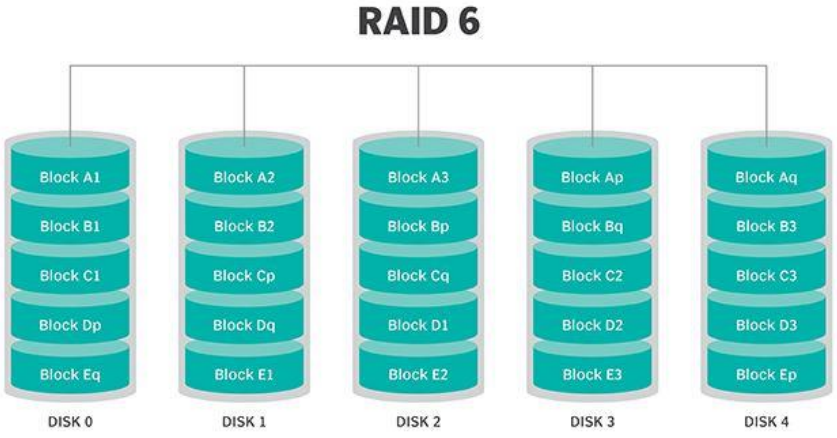
RAID 5 využíva delenie dát na blokovej úrovni a to spolu s paritou na každom disku. Týmto delením je eliminovaný problém, ktorý sa vyskytuje u RAID 4 a tým je pomalší zápis. Rozdelením parity medzi všetky disky je problém vyriešený a zápis je rýchlejší. RAID 5 je najpoužívanejším usporiadaním diskového poľa a to najmä z dôvodu jeho rýchlosti a dostupnosti. Toto pole vyžaduje využitie minimálne troch diskov. Výhodou tohto typu RAID je, že spôsob delenia dát a parít zabraňuje spomaľovaniu procesu zápisu/ čítania ktorýmkoľvek z diskov. Ide o jeden z najbezpečnejších usporiadaní RAID, poskytuje kvalitnú redundanciu rovnako ako spoľahlivosť. Disky môžu byť Hot-Swapped, čo znamená, že môžu byť vymenené za chodu, čím je eliminovaný prestoj. Nevýhodou je, že zápis je rýchlejší ako čítanie z dôvodu prepočtu dát parity. Vyžaduje komplikovanejší ovládač. Ďalšou nevýhodou je dlhší čas obnovy a možná strata dát v prípade, že sa v tomto procese pokazí druhý disk. Najlepšie využitie tohto úložného poľa je pre aplikačné alebo súborové servery s obmedzeným počtom diskov. Schéma úložisko RAID 5 je znázornená na Obr. 1.6 [7].



Obr. 1.6: Schéma úložiska typu RAID 5; block – blok, parity – parita, block parity – bloková parita [7]

1.3.7 RAID 6

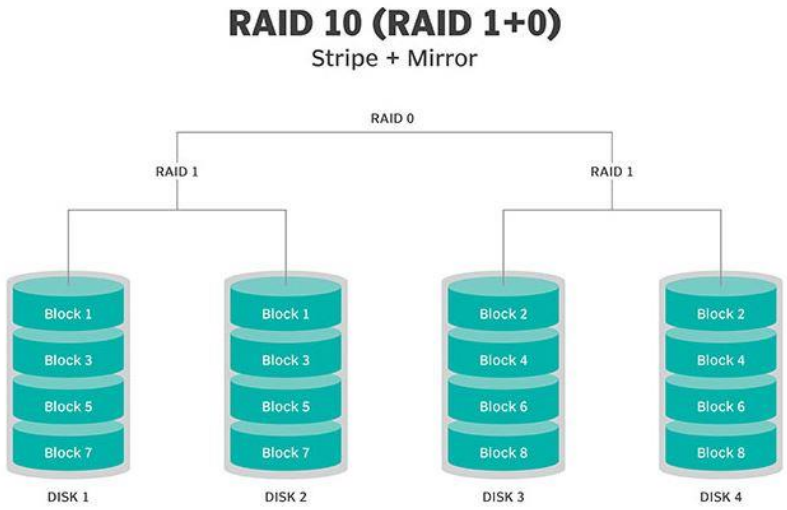
RAID 6 je usporiadanie (zobrazené na Obr. 1.7), pri ktorom sú dáta ukladané na viacero diskov, pričom sú povolené input/output operácie. Tieto operácie predstavujú zásahy pre vyvážený chod systému a tým nepriamo zlepšujú výkon. V poli RAID 6 sa parity rozdeľujú do dvoch blokov čím je umožnená funkčnosť systému aj pri zlyhaní dvoch diskov predtým, ako dôjde ku strate dát. Umožňuje obnovu dát počas súčasného zlyhávania diskov. Konfigurácia RAID 6 vyžaduje najmenej 4 disky. Výhodou je poskytnutá ochrana v prípade zlyhania druhého disku. Percento využiteľnej kapacity stúpa postupným pridávaním diskov do poľa. Pri využití viac ako štyroch diskov pole využíva menej kapacity, ako je tomu pri poli RAID s nastaveným zrkadlením. Nevýhodou je nižší výkon v porovnaní s RAID 5. Obnova je výrazne spomalená pri nutnej obnove dvoch diskov súčasne. Z dôvodu potreby 2 diskov pre parity je navýšená cena. Je tu aj potreba využitia špecializovaného ovládača a taktiež pre zvýšenie výkonu pri výpočte parít a zrýchlenie zápisu je potrebný koprocesor ovládača RAID. RAID 6 je teda vhodný pri nutnosti dlhodobého uchovania dát alebo v kritických oblastiach z dôvodu jeho schopnosti vysokej ochrany dát [7].



Obr. 1.7: Schéma úložiska typu RAID 6; block – blok [7]

1.3.8 RAID 10

Redundantné pole nezávislých diskov RAID 10 je kombináciou viacerých zrkadlených diskov s rozdelením dát do blokov v jednom poli. Pole RAID 10 je zložené z minimálne 4 diskov, pričom sú vytvárané sety pozostávajúce z párov zrkadlených diskov. V rámci zrkadlených diskov sú dáta usporiadané blokovo. Môže byť označovaný aj ako RAID 1+0. Základným konceptom je spájanie kapacitne menších diskov do jedného veľkého poľa, ktoré poskytuje výkonné a voči chybám odolné vlastnosti. Výkon poľa RAID 10 tak často presahuje výkon jedného drahého disku. Mechanizmus zahŕňa rozdeľovanie dát medzi všetky zrkadlené celky. Ako to už bolo diskutované pri poli RAID 1, zväčša sú zahrnuté iba 2 disky, aj keď je možné využitie viacerých diskov. RAID 0 postupne rozdeľuje dáta medzi viaceré disky. RAID 10 duplikuje alebo zrkadlí prvé dva disky v celku. Výsledkom je vysoký výkon a zvýšená ochrana údajov. Výhodami poľa RAID 10 sú: vysoký výkon; redundancia dát, pomer zapisovania a čítania; tolerancia zlyhania. Nevýhodami sú: náročné nastavenia a vyššia cena riešenia. Celková dostupná kapacita je polovica zo súčtu veľkosti kapacít jednotlivých diskov v poli a to z dôvodu delenia dát medzi zrkadlené disky. Schému RAID 10 vidíme na Obr. 1.8 [7,8].



Obr. 1.8: Schéma úložiska typu RAID 10; stripe - rodeľovanie, mirror - zrkadlenie block – blok [7]

1.4 Zálohovacie médiá

HDD

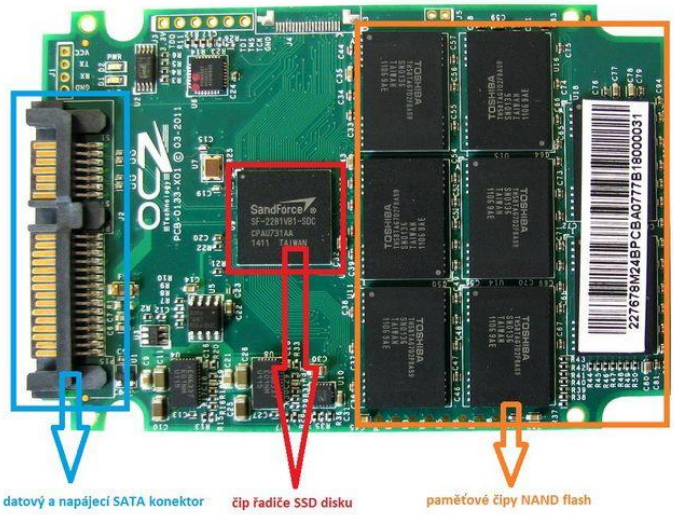
Zariadenie určené na ukladanie dát, ktoré sú ukladané na vysokootáčkové magnetické disky. Disky sú roztáčané elektromotorom stabilnou rýchlosťami štandardne 4200, 5 400, 7 200, 10 000 alebo 15 000 otáčok za minútu. Rýchlosť zápisu a čítania je daná počtom otáčok za minútu. Disky sú uzatvorené v obale odolnom voči prachu. Na samotné čítanie a zápis dát z diskov sú využívané zapisovacie a čítacie hlavy, ktoré sa nachádzajú na pohyblivých ramenách. Pevné disky delíme podľa využitia, či už v počítači alebo notebooku, na 3,5 alebo 2,5 palcové. HDD sa využívajú ako externé alebo interné disky. Externé disky sú prenositeľné a majú možnosť pripojenia k počítaču alebo inému zariadeniu prostredníctvom

USB. Interné disky sú súčasťou počítača a sú pripájané pomocou ATA, SCSI alebo SATA rozhrania. Súčasťou HDD je platňa diskového tvaru s naneseným magnetickým materiálom, ktorá je rotujúcou časťou. Nad platňami sa pohybuje magnetická hlava, ktorá zapisuje alebo číta dáta, ako je zobrazené na Obr. 1.9. Elektronická časť disku slúži na prenos signálov, v ktorých sú kódované informácie. Disk je rozdelený na stopy. Jednotlivé stopy sú ďalej delené na sektory. Sektor je najmenšia adresovateľná jednotka disku, obvyklá veľkosť sektora je 512 bitov [9].

Obr. 1.9: Vnútorná stavba pevného disku [9]

SSD

Na rozdiel od HDD, SSD disk (zobrazený na Obr. 1.10) nemá žiadne pohyblivé časti, čo prináša výhody rýchlejšieho prístupu k dátam, tiché fungovanie, vyššiu spoľahlivosť a nižšiu spotrebu energie. Dáta sú ukladané do flash pamäte typu NAND. NAND sú sústavou logických hradiel, kde sú logicky zapísané dáta. Dôležitým prvkom SSD disku je radič, ktorým býva čip MLC (Multi-Level Cell) alebo SLC (Single-Level Cell). Radič je zodpovedný za algoritmizáciu zápisu, ktorá sa medzi typom MLC a SLC líši. Obmedzenie počtu zápisov je dané práve použitím čipu SLC alebo MLC. U SSD klesá výkon s množstvom uložených dát. Podľa rozhrania ich delíme na: mSATA, M.2 alebo PCIe. Vyrábajú sa štandardne v rozmeroch 1,8 a 2,5 palca. V poslednej dobe ich cena výrazne klesla a tak sú ideálnou náhradou HDD v počítačoch alebo notebookoch. Nevýhodou je pokles výkonu opotrebením, obmedzený počet zápisov a nemožnosť obnovy dát [10,11].



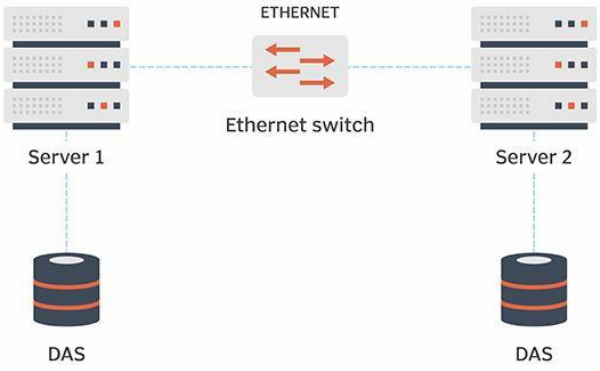
Obr. 1.10: Vnútorná stavba SSD disku [11]

1.5 Dátové úložiská

Dátové úložisko môže byť navrhnuté v rôznych topológiách, ktoré sa líšia svojim účelom a štruktúrou prevedenia. Rôzne topológie poskytujú odlišné praktické vlastnosti.

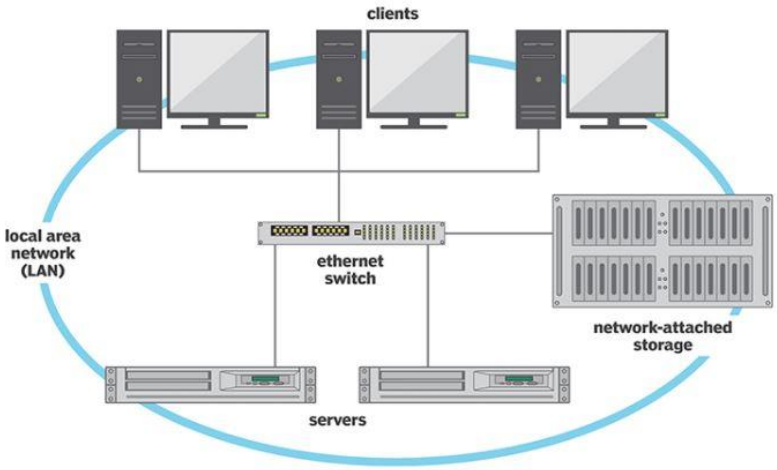
1.5.1 Topológia dátových úložísk

DAS – je úložisko priamo spojené (direct-attached storage) s počítačom, ktoré nie je prístupné iným zariadeniam. Ako DAS je zvyčajne označovaný HDD alebo SSD disk. Filozofia tohto úložiska je opačná voči konceptu úložísk prístupným cez počítačovú sieť. DAS je typicky tvorený dátovým nosičom, ktorý je s počítačom spojený pomocou HBA (Host Bus Adapter). Medzi týmito úložiskami nie je žiadne sieťové zariadenie, schéma topológie je zobrazená na Obr. 1.11 [12].



Obr. 1.11: Topológia úložiska DAS; switch – prepínač [12]

NAS – dátové úložisko na sieti (network-attached storage) umožňuje získavanie a ukladanie dát z/na centralizované úložiská viacerým užívateľom a heterogénnym zariadeniam. Užívatelia na lokálnej sieti pristupujú k zdieľanému úložisku cez štandardné ethernetové pripojenie. Každé zariadenie NAS je na LAN sieti ako nezávislý sieťový uzol definovaný svojou unikátnou IP adresou. Dátové úložisko NAS, ktorého schéma je na Obr. 1.12 je často využívané ako základ pre súkromné cloudové úložisko [13].



Obr. 1.12: Topológia úložiska NAS; clients – klienti; local area network – lokálna sieť, servers – servery, ethernet switch – ethernetový prepínač, network-attached storage – dátové úložisko na sieti [13]

SAN – je vyhradená vysokorýchlostná dátová sieť alebo podsieť (storage-attached network), ktorá prepája zdieľané dátové sklady zariadení ku viacerým serverom. Dostupnosť a prístupnosť úložiska sú kritickými požiadavkami pre operácie v spoločnosti. Topológia SAN, znázornená na Obr. 1.13, umožňuje, aby spoločnosť narábala s úložiskom, ako jedným celkom zdrojov, ktorý môže byť centrálne replikovaný alebo chránený. Prídavné technológie, ako napríklad RAID optimalizujú kapacitu úložiska a výrazne zvyšuje odolnosť úložiska v porovnaní s DAS [14].

Obr. 1.13: Topológia úložiska SAN; SAN switch – SAN prepínač, Fibre Channel – optický kanál [14]

1.5.2 Sieťová infraštruktúra

Sieťová infraštruktúra predstavuje kostru, ktorá podporuje systém alebo organizáciu a to aj v zmysle prístupu a zdieľania dátových úložísk. Je zložená z fyzických a virtuálnych zdrojov podporujúcich tok, úložisko, spracovanie a analýzu dát. Infraštruktúra môže byť centralizovaná v rámci dátového centra alebo môže byť rozdelená medzi viacero dátových centier, ktoré sú kontrolované spoločnosťou, ako je napríklad cloud provider [14].

1.6 Cloudové dátové úložiská

Hybridný – prístup k spravovaniu cloudového úložiska využívajúceho lokálne a externé zdroje. Infraštruktúra hybridného cloudového úložiska je často využívaná ako doplnok interného úložiska s verejným cloudovým úložiskom. Softvéry politiky nechávajú často využívané dáta na mieste a zároveň presúvajú dáta neaktívne na cloudové úložisko transparentným spôsobom. Hybridné cloudové úložisko je obvyklý spôsob, ktorým spoločnosti sprostredkovávajú zálohu dát a ich obnovu v prípade straty. Ďalším častým využitím tohto cloudového úložiska je oddelenie archívov a zriedka využívaných dát od pravidelne využívaných dát [15].

Verejné – ide o model služby, ktorá poskytuje platené dátové úložisko verejne prístupné cez internet. Poskytované zdroje zahŕňajú kapacity úložiska a využitie aplikácií alebo virtuálnych systémov. Zvyčajne je verejné cloudové úložisko spoplatnené na základe množstva využívaných dát. Taktiež sa často platí za presun dát z alebo na cloud, takže presun dát a prístup

k nim, môže navýšiť cenu za služby cloudového úložiska. Výhodou verejného cloudového úložiska je, že cena je účtovaná len za využívanú kapacitu. Na rozdiel od toho je inštalácia vlastného úložného priestoru spoločnosťou platená aj v prípade, že celá kapacita nebude využitá. Celá kapacita vlastného úložiska nebýva využívaná, nakoľko zvyšovaním využívanej kapacity často klesá výkon. Zvyšovanie alebo znižovanie kapacity miestneho dátového úložiska je taktiež nákladnejšie a komplikovanejšie. Veľkou výhodou je možnosť jednoduchého zdieľania dát. Nevýhodou je často vyžadované potvrdenie poskytovateľom pre prístup k dátam na cloude. Pokiaľ chce spoločnosť k dátam pristupovať inak, ako len priamo cez internet, tak táto zmena prístupu môže byť nákladná. Nevýhodou môže byť aj možná strata dát v procese prenosu, v prípade výpadku u providera a tiež bezpečnostné riziko súvisiace s neoprávneným prístupom k dátam [16].

Privátny – cloudové úložisko funguje na dedikovanej infraštruktúre v dátovom centre, ponúkajúc rovnaké výhody škálovateľnosti verejného cloudového úložiska, pričom rieši aj bezpečnostné a výkonnostné problémy. Požiadavky škálovateľnosti pre privátne cloudové úložisko sú jednoduchšie v porovnaní s verejným cloudovým úložiskom a to z dôvodu, že základňa užívateľov pre privátne cloudové úložisko je zvyčajne limitovaná pre skupiny v rámci organizácie. Verejné cloudové úložisko môže mať milióny potenciálnych užívateľov využívajúcich túto službu. Privátne cloudové úložisko je preto vystavané na základe tradičného dátového úložiska. Pri využívaní tohto typu cloudového úložiska môže byť organizácia požiadaná o uchovávanie niektorých dát na miestnom úložisku z dôvodu ich ochrany [17].

1.6.1 Virtualizácia

Virtualizácia dát je výraz popisujúci prístup k správe dát, ktorý umožňuje aplikovanie obnovy a manipulácie dát bez potreby detailov o dátach, ako napríklad spôsob, ktorým sú dáta formátované, alebo kde sa fyzicky nachádzajú. Cieľom virtualizácie dát je vytvorenie jedného zastúpenia dát z viacerých, fyzicky a logicky nezlúčiteľných zdrojov. Pritom nevzniká potreba kopírovania alebo presunu dát. Virtualizácia v tomto zmysle predstavuje technológiu pre organizáciu zdrojov. Umožňuje užívateľom využívať zdroje efektívnejším spôsobom a to z pohľadu fyzickej kapacity tak aj softvérových procesov. Podľa spôsobu realizácie sa rozdeľuje na plnú virtualizáciu, paravirtualizáciu a hardvérovú virtualizáciu. Pri plnej virtualizácii je požiadavka formulovaná OS a príslušným hardvérom hostiteľa konvertovaná na úroveň vyššej inštancie. Takto je dosiahnutá dobrá kompatibilita využitia zdrojov aj bez potreby zmien v OS hostiteľa. Technológia paravirtualizácie pridáva špecifické inštrukcie pre OS hostiteľa a tieto inštrukcie priamo oslovujú hardvérové prostriedky prostredníctvom nadradenej vrstvy. Tento typ virtualizácie už vyžaduje určité zmeny v OS hostiteľa. Posledným typom je hardvérová virtualizácia, ktorá je poskytovaná výrobcami hardvéru, najčastejšie využívaná spoločne s plnou alebo paravirtualizáciou. Ide o operatívny mód, ktorý nastavuje nové inštrukcie pridané do jednotky procesora (CPU). Príkladom tejto technológie je Intel VT alebo AMD-V [18,19].

1.6.2 Cloud computing

Termín označujúci čokoľvek súvisiace s poskytovaním hostovaných služieb cez internet. Tieto služby sú rozdelené do troch hlavných kategórii: infraštruktúra ako služba (IaaS), platforma ako služba (PaaS) a softvér ako služba (SaaS). Cloud môže byť privátny alebo

verejný. Verejný cloud ponúka služby komukoľvek na internete. Privátny cloud je súkromná sieť alebo dátové centrum, ktoré zásobuje hostované služby limitovanému počtu ľudí s určitými právami a nastaveniami povolení. V oboch typoch cloudu je cieľom cloud computingu poskytovanie jednoduchého a škálovateľného prístupu ku výpočtovým zdrojom a IT službám. Cloudová infraštruktúra obsahuje hardvérové a softvérové prvky požadované pre správnu implementáciu modulu cloud computingu [20].

IaaS – poskytovanie inštancie a úložiska virtuálneho servera. Infraštruktúra ako systém taktiež poskytuje API, ktoré umožňujú užívateľom presun hardvérovej záťaže na virtuálny stroj. Užívatelia majú priradenú kapacitu úložiska a môžu spustiť, zastaviť, pristupovať alebo konfigurovať virtuálny stroj a úložisko podľa vlastného uváženia [20].

PaaS – cloud provideri hostujú vývojové nástroje na svojej infraštruktúre. Užívatelia pristupujú k týmto nástrojom cez internet pomocou API, webových portálov alebo gateway softvéru. Platforma ako služba je využívaná pre všeobecný vývoj systému a množstvo PaaS providerov hostuje softvér po ukončení jeho vývoja [20].

SaaS – modelová distribúcia poskytujúca softvérové aplikácie cez internet. Tieto aplikácie sa nazývajú webové služby. Užívatelia môžu pristupovať k SaaS aplikáciám a službám z akejkoľvek lokácie pomocou počítača alebo mobilného zariadenia s prístupom na internet. V tomto modeli užívatelia získavajú prístup k aplikačným softvérom a databázam [20].

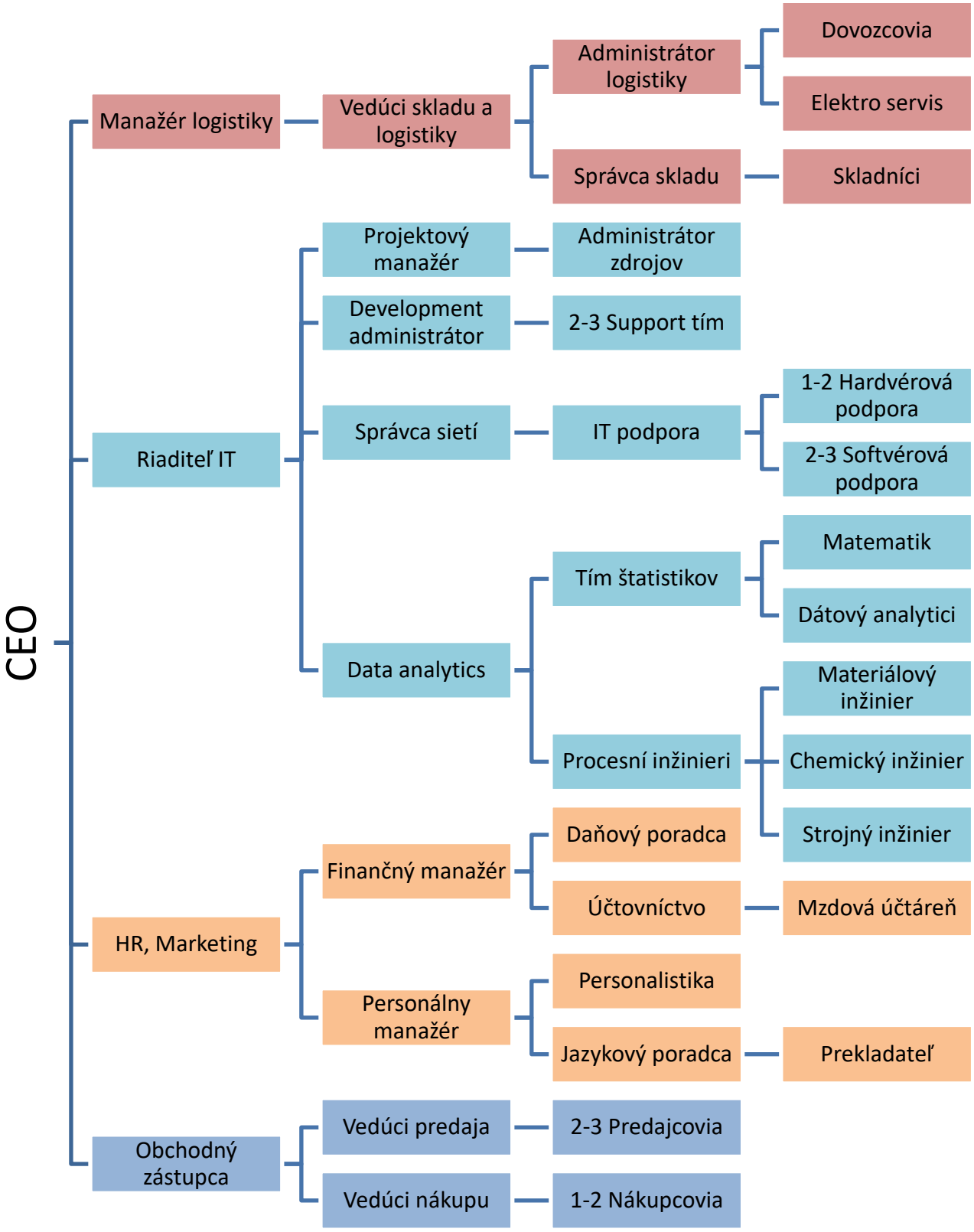
2 ANALÝZA SÚČASNÉHO STAVU

V rámci bakalárskej práce analyzujem a riešim informačnú bezpečnosť z pohľadu zálohovania a návrhu dátového úložiska pre spoločnosť Prinet s.r.o., ktorá podniká v oblasti senzorovej techniky, v segmente IoT (Internet of Things) a zároveň spravuje dáta zákazníkov, za účelom nastavenia a zabezpečenia výrobných systémov vo svojich firemných databázach. Prvým krokom analýzy je získanie informácii o spoločnosti, preskúmanie organizačnej štruktúry a vzájomných vzťahov v spoločnosti. V nasledujúcich podkapitolách to je analýza softvérových a hardvérových prostriedkov spoločnosti. Ďalšou dôležitou časťou analýzy je stanovanie sieťovej infraštruktúry, sieťových prvkov, vzájomných väzieb, dátových tokov, tieto sú zhrnuté v podkapitole počítačová sieť spoločnosti. V poslednej podkapitole je riešený proces a systém zálohovania dát rôznej priority spoločnosti. Dôležitým krokom je tiež analýza rizík a posúdenie následkov a úrovne rizika.

2.1 Základné informácie a organizačná štruktúra spoločnosti

Spoločnosť Prinet s.r.o., ktorá aktívne pôsobí od roku 2016, je firma regionálneho významu pôsobiaca v oblasti IT, zaoberajúca sa analýzou IoT dát. Spoločnosť inštaluje u svojich zákazníkov senzory, ktoré sledujú výrobné a technické procesy zákazníkov. Senzory zbierajú dáta, ktoré spoločnosť vyhodnocuje a zákazníkom ponúka spätnú väzbu na zmeny v ich procesoch alebo navrhuje optimalizácie procesov. V súčasnosti má spoločnosť 28 stálych zamestnancov, ktorí pracujú v rámci štyroch oddelení: oddelenie logistiky, IT oddelenie, oddelenie HR a marketingu a v obchodnom oddelení. Firma je svojou veľkosťou malá, preto niektorí zamestnanci zastupujú viaceré pozície.

Organizačná štruktúra spoločnosti je schematicky uvedená na Obr. 2.1. Spoločníci z valnej hromady spoločnosti zvolili na základe spoločenskej zmluvy jedného generálneho riaditeľa, ktorý je konateľom firmy v schéme uvedený ako CEO (Chief Executive Officer), ktorý je priamym nadriadeným manažérov jednotlivých oddelení: manažérovi logistiky, riaditeľovi IT, marketingovému a HR manažérovi a obchodnému zástupcovi. Títo manažéri hierarchicky zodpovedajú za svojich podriadených.



Obr. 2.1: Organizačná štruktúra spoločnosti Prinet s.r.o.

2.2 Softvérové prostriedky

V tejto kapitole sú diskutované softvérové nástroje od všeobecnej úrovne inštalovaného OS (Operačný systém) a kancelárskych balíkov, špeciálneho softvéru pre potreby jednotlivých oddelení napr. logistika, financie a marketing, až po úroveň profesionálnych nástrojov určených pre hlavnú činnosť spoločnosti – analýzu dát.

2.2.1 OS a kancelárske balíky

Pracovníci majú najčastejšie k dispozícii notebooky, kde je nainštalovaný OS Microsoft Windows 10, taktiež je na štyroch PC nainštalovaný OS Microsoft Windows 7. Na všetkých počítačoch je nainštalovaný licencovaný kancelársky balík Microsoft Office 365, ktorý je najuniverzálnejším a taktiež najčastejšie využívaným softvérovým balíkom, konkrétne MS Word, MS Excel, MS PowerPoint a MS Outlook. Na jedinom vlastnom serveri spoločnosti je nainštalovaný OS Linux.

2.2.2 Špeciálny softvér

Účtovníci využívajú ekonomický program **Pohoda** v slovenskej verzii. Na riešenie skladových zásob, návrh objednávok a sledovanie zariadení pridelených projektom slúži softvér **BMD Business**. Pre technické účely a technické správy je využívaný prekladateľský softvér **Lingea 6.0**. Softvér pre dátovú analýzu **Statistica 14.0** od firmy TIPCO a **MATLAB 9.4** od firmy MathWorks. Pre vizualizáciu a predikčné modely dát využíva softvérový nástroj **Elastic licenciu 2.0**.

2.3 Hardvérové prostriedky

Osobitne sú v kapitole rozdelené hardvérové prostriedky pre osobné pracovné stanice a súčasné sieťové prvky spoločnosti, ktoré zahŕňajú aj výkonný hardvér pre dátovú analýzu.

2.3.1 Osobné počítače a kancelárske vybavenie

Pre kancelárske použitie disponuje firma 15 kusmi laptopov značky **Lenovo, model Yoga C640-13IML** s dotykovou obrazovkou, technické parametre sú uvedené v Tab. 2.1.

Tab. 2.1: Technické parametre Lenovo Yoga C640

Procesor	4 jadrový Intel Core i5-10210U
Pamäť RAM	8GB DDR4
Pevný disk	512 GB SSD
Grafická karta	Integrovaná Intel UHD Graphics

Firma má aj 5 kusov starších laptopov **Lenovo IdeaPad 3 15IIL05**, technické parametre sú uvedené v Tab. 2.2.

Tab. 2.2: Technické parametre Lenovo Ideapad 3

Procesor	Intel Core i3 1005G1
Pamäť RAM	8GB DDR4
Pevný disk	256 GB SSD
Grafická karta	Integrovaná Intel UHD Graphics

Komplexné tlačové služby sú zabezpečované outsourcingom pomocou externej firmy, ktorá poskytuje tlačiarne **Canon imageRUNNER C3125i**. Okrem komplexných tlačových služieb sú v kanceláriách inštalované jednoduché laserové tlačiarne **HP LaserJet Pro MFP M28w**.

2.3.2 Sieťové prvky

Aktuálne je v serverovni k dispozícii zariadenie NAS server lokálnej siete **Synology DS1621+**, ktorý obsahuje 6x **SSD Samsung DCT 960GB** (technické parametre sú v Tab. 2.3), okrem toho sú vo firemnej sieti 3 routre, profesionálny firemný router s Gigabit ethernet pripojením **CISCO2911/K9** a dva WIFI routre **TP-LINK Archer AX20**, ďalej switche pre serverovňu 2x **Cisco SX350X-08-K9-EU** a v kanceláriách 2 switche **Ubiquiti US-24-250 W**. Pre prípad výpadku energie je obstaraný záložný zdroj UPS **APC Smart-UPS SRT 10000 VA RM 230 V**, ktorý slúži na rýchle ukončenie dôležitých procesov a prípadné uloženie dôležitých dát počas výpadku.

Tab. 2.3: Parametre serveru NAS a jeho diskových jednotiek

Server **Synology DS1621+**	
Procesor	Ryzen V1500B 2,2 GHz
Pamäť RAM	4GB DDR4
Operačný systém	Windows Server 2012
Diskové jednotky **Samsung DCT 960GB**	
Rýchlosť zápisu	520 MB/s
Rýchlosť čítania	550 MB/s
Rozhranie	SATA III

2.3.3 Výkonné zariadenia pre analýzu dát

Server **DELL PowerEdge R740** (technické parametre sú v Tab. 2.4) je výkonným výpočtovým zariadením, na ktorom sú zdieľané analytické nástroje a pracovníci môžu pomocou neho vykonávať sofistikované operácie s dátami. Iba v lokálnej sieti sa mapuje ako //analytics.

Tab. 2.4: Parametre výkonného serveru DELL PowerEdge R740

Procesor	Intel Xeon Gold 5218 16 jadro
Pamäť RAM	4x 32GB DDR4
Pevný disk	480 GB SSD SATA III
Operačný systém	Red Hat Enterprise Linux 7.4

2.4 Cloudové úložisko

Nateraz spoločnosť uchováva a spravuje väčšinu dát formou cloudu od firmy Sincplicity. V prenájme je typ hybridného úložiska, ktorý kombinuje služby súkromného a verejného cloudu a dáva spoločnosti možnosť zvoliť si, aký typ dát bude smerovaný do súkromného a verejného priestoru. Momentálne sú súčasťou verejného priestoru menej citlivé dáta, ako sú maily, služobná komunikácia prostredníctvom komunikačnej platformy MS Teams, rozpracované menej dôležité projekty, ktoré neobsahujú utajované skutočnosti. Do súkromného cloudu sú smerované dáta získavané od zákazníkov, obchodné tajomstvá, zmluvy a utajované právne dokumenty. Nastavená služba v súčasnosti umožňuje prístup k dátam zo zariadení založených na rôznej platforme, používané rozhranie je relatívne prehľadné, je umožnené sledovanie používania obsahu od rôznych používateľov. Administrátor má široké možnosti implementovať zásady a kontrolu prístupu k údajom, ďalej má možnosti vytvárať skupiny používateľov a poskytovať im rôzne práva a aktívne ovládacie prvky. V súčasnosti spoločnosť využíva najnižší možný program pre malé podniky, ktorý má tarifu 60 USD/používateľ ročne. Zvolený program cloudu od Syncplicity je uvádzaný ako business edition, ktorého súčasťou je práve administratívna kontrola a kontrola prístupu, nastavovanie politík skupín užívateľov a manažment pripájaných zariadení. Zároveň je administrátor schopný obmedziť nahrávanie súborov podľa typu a zdieľanie súborov s užívateľmi mimo spoločnosti. Súčasťou technického riešenia je:

- Sledovanie, zabezpečenie a organizovanie dát spoločnosť rieši interne a úplne samostatne. Syncplicity ponúka cloud úložisko, čo znamená, že si spoločnosť zabezpečuje taktiež bezpečný prenos dát. Kritické je správanie vlastníkov dát z pohľadu prevencie straty a obmedzenia webových služieb.
- Možnosť zmeny koncového úložiska dát určeným administrátorom. Súkromné dátové úložiská môžu využívať ktorékoľvek dátové pole podporujúce dátové úložisko na sieti (NAS, Network Attached Storage) alebo objektové úložisko. Pre NAS je k dispozícii prístup cez NFSv3 (Network File System verzia 3.), pristupovať je tak možné k systémom tretích strán. Pre objektové úložiská je možné využiť polia Atmosu alebo EMC ECS. Na prepojenie s AWS je využitý konektor Syncplicity On-Premise, ktorý predstavuje softvér fungujúci ako virtuálny operátor, spájajúci koncové úložiská. Zvyšuje sa tak škálovateľnosť a dostupnosť úložiska. Na vyrovnávanie prenosovej záťaže sa využíva protokol SSL (Secure Sockets Layer).
- Z pohľadu bezpečnosti je dôležitá autentifikácia užívateľa, tá je konfigurovaná pomocou protokolu SSL medzi konektorom úložiska a vlastnou službou individuálneho prihlásenia SSO (Single Sign-on) napr. služba štandardu SAML 2.0 (Security Assertion Markup Language verzia 2.0).

- Veľkosť kapacity úložiska je daná zakúpeným účtom Data Protection Suite, ktorý slúži aj na prerozdeľovanie kapacity úložiska medzi úplne súkromné a založené na cloude. Možno nakonfigurovať veľkosť kapacity priradenej len pre súkromné účely a veľkosť pre cloud. Avšak správy o výstupoch z uložených súborov sú vždy exportované na cloud, preto treba zachovávať dostatočnú rezervu na cloude. Spoločnosť má zakúpených 5 TB, z toho cloudovo prístupné sú 2 TB.
- Využívanie metadát na označovanie súborov alebo priečinkov (tagging), je nevyhnutná vlastnosť, ktorú aktivuje administrátor spoločnosti. Toto riešenie Syncplicity umožňuje a spoločnosťou je na triedenie dát nastavená politika, ktorá dáta prioritizuje podľa dôležitosti a tiež im priraďuje atribúty, podľa ktorých je možné zistiť pôvod, typ a vek súborov. Udalosti spojené s tagovaním sú ukladané v auditorských správach.
- Spoločnosť má v rámci tohto riešenia systém s prevenciou straty dát DLP (Data Loss Prevention), s možnosťou konfigurovať vlastné DLP politiky. DLP zároveň klasifikuje dáta z historického hľadiska, t. j. možno určiť vek chránených dát, typ súborov, tiež je možné nastaviť veľkosť chránenej časti úložiska a sledovať správanie užívateľov z pohľadu DLP klasifikácie resp. zamietnuť alebo obmedziť prístup.

2.5 Zálohovanie dát

Zálohovanie je aktuálne majoritne riešené cloudovým úložiskom, pre ktoré platia nastavené politiky spomínané v kap. 2.4. Okrem toho sa v malej miere využíva NAS server Synology DS1621+, kde sú uchované nedokončené projektové dáta vývojových tímov alebo nedôležité dokumenty oddelenia marketingu a HR, ktoré sú v štádiu rozpracovania. Ukladať hotové projekty a finálne dokumenty len na tento server je firemnou politikou zakázané, v tomto prípade sa musí využiť cloud. Zálohovanie v cloude je nastavené na dennej báze a denne sú o zálohovaní a ukladaní dát vystavované reporty, ktoré prichádzajú na mail administrátorovi IT oddelenia.

2.5.1 Zálohovanie pracovných staníc

Politika prístupu na NAS server je dopredu definovaná a tak každý prijatý zamestnanec dostane prístupové práva do lokálnej siete cez doménu nastavenú na OS Windows. Jednotlivci majú definované svoje vlastné užívateľské práva v rámci domény. Základným právom a podľa firemnej politiky aj povinnosťou je prístup read/write s obmedzením na mazanie dát k lokálnemu NAS serveru. Úplné práva k NAS serveru a dátam uloženým na tomto serveri majú správcovia sietí. Na serveri je viac úrovní vzhľadom k typu dát. Všetci užívatelia majú základný prístup k priečinku \\general. Tento priečinok si je povinný každý zamestnanec namapovať. Ďalej je vytvorený priečinok \\internal, ku ktorému majú prístup užívatelia z oddelenia účtovníctva a obsahuje ako faktúry tak aj výplatné pásky. Pre správcu a skladníkov je zavedený priečinok s názvom \\warehouse. Priečinok obsahuje informácie týkajúce sa skladových zásob. Na základe požiadavky riaditeľa IT vznikol priečinok \\projects, kde sú zálohované rozpracované projektové súbory pred finálnym ukončením pre zamestnancov, ktorí spadajú pod IT časti.

2.5.2 Zálohovanie NAS serveru

Toto zariadenie je zálohované s frekvenciou raz týždenne formou inkrementálnej zálohy. Prevádza sa externá záloha na SSD Samsung Portable T7 Touch s kapacitou 2TB, ktoré disponuje biometrickými ochrannými prvkami. Funkcia Touch ID je využívaná na odblokovanie zariadenia. SSD má v serverovni vyčlenené miesto a majú ku nemu prístup iba osoby určené, tými sú: CEO, riaditeľ IT a správca sietí. Dáta sú zálohované na dobu pol roka. Pred ich vymazaním sú všetci zamestnanci o tejto skutočnosti oboznámení pre prípad, že by niektoré dáta ešte potrebovali. Dáta sú komprimované s rôznymi úrovňami komprimácie a to bezstratovú a stratovú. So zvolenými kompresnými pomermi podľa uváženia zodpovedného technika a charakteru dát.

2.5.3 Software na zálohovanie

Softvérové nástroje od Syncplicity, kde má administrátor práva presmerovania a zoskupovania dát do jednotlivých blokov privátnej a verejnej časti cloudu, s nastavením povinného využívania metadát k popisu vlastných dát a systémom DLP politiky.

Na osobné počítače a server lokálnej siete je aplikovaný softvér Paragon, ktorý ponúka ochranu dát a vytváranie automatizovanej zálohy. Okrem pravidelného zálohovania označených priečinkov osobných PC zamestnancov je softvér využívaný na vytváranie bootovacích USB diskov alebo spustiteľnej zálohy pre prípad fatálneho zlyhania operačného systému.

S využívaním nástrojom MS Teams a sady MS Office je čiastočne pri práci využívané aj cloudové riešenie spoločnosti Microsoft MS OneDrive, táto záloha však nie je systémovo organizovaná.

2.5.4 Zálohovanie na cloude

Všetky zálohy na cloude sa nachádzajú v privátnej časti cloudu, t. j. v súčasnosti 5TB kapacity a z toho sú pre zálohu vyčlenené až 3TB. Verejná časť cloudu je zo zálohovania dát vyčlenená, t. j. nemôžu sa tam dávať dáta, ktoré je nevyhnutné zálohovať. Nevyhnutnou vlastnosť zálohy na cloude, ktorá je aktivovaná administrátorom spoločnosti, je využívanie metadát a označovanie súborov alebo priečinkov (tagging). Tento proces je pre zamestnancov definovaný v interných smerniciach a dáta musia byť povinne klasifikované. Určený administrátor má možnosť zmeny koncového úložiska dát, t. j. aj prenos dát z cloudu na lokálne zálohy. Na prácu s dátami na cloude je nutné prejsť procesom autentifikácie užívateľa. Využíva sa systém s prevenciou straty dát DLP s možnosťou nakonfigurovania vlastnej DLP politiky.

2.5.5 Proces zálohovania

Proces zálohovania sa riadi prísne nastavenou firemnou politikou vzhľadom k tomu, že spoločnosť disponuje aj citlivými dátami od zákazníkov, je vyžadované dodržiavanie zavedených pravidiel. Súhrnne je možné tieto pravidlá formulovať ako požiadavky na kategorizáciu a prioritizáciu dát do dátových celkov, pričom od určitej priority je pre operácie s dátami zavedený proces krížovej kontroly a práva nad týmito operáciami sú dané len zodpovedným administrátorom dát. Dáta sú rozdelené do dátových celkov obsahujúcich

informácie rôzneho určenia a významu, s ktorými disponujú určití pracovníci. Kategorizáciou je myslené stanovenie a určenie pôvodu, typu a veku dát.

Základnou kategóriou je typ dát. V spoločnosti boli zavedené nasledujúce typy dát, s ktorými operujú rôzni pracovníci a sú súčasťou rozličných firemných procesov: dáta od zákazníkov; projektové dáta; dokončené a rozpracovane projekty; reporty z dátovej analýzy; manažment a marketing; účtovníctvo; údaje o zamestnancoch a logistika, pod ktorú spadajú skladové zásoby a doprava.

Prioritizácia potom predstavuje vytvorenie skupín dát podľa jednotlivých kategórii, ktorým je priradený rôzny stupeň ochrany na základe dohodnutej bezpečnostnej politiky spoločnosti. Priorita je označená od najnižšej (A) až po najvyššiu (E). Priorita je tiež určená vekom jednotlivých dát. Zjednodušený popis narábania s dátami podľa priority a kategórie v spoločnosti je uvedený v Tab. 2.5.

Tab. 2.5: Kategorizácia a prioritizácia dát

Typ dát	Vek	Priorita	Zodpovedný správca	Dotknutí pracovníci
Dáta od zákazníkov	Mesiac až rok	E - C	Riaditeľ IT	Dátový analytici, matematik
Projektové dáta dokončené	Mesiac až >rok	E - B	Projektový manažér	Projektový manažér, Administrátor zdrojov
Projektové dáta rozpracované	Týždeň až >mesiac	E	Projektový manažér	Projektový manažér, Administrátor zdrojov
Reporty z dátovej analýzy	Týždeň až >mesiac	D	Dátový analytik	Tím štatistikov, matematik, dátový analytik
Manažment a marketing	Mesiac až m>rok	B - C	Personálny manažér	Personálny manažér , personalisti
Účtovníctvo	Týždeň až >rok	D	Finančný manažér	Účtovník, mzdový účtovník
Údaje o zamestnancoch	Mesiac až >rok	C - D	Personálny manažér	Personalisti
Logistika	Týždeň až rok	C - A	Manažér logistiky	Vedúci skladu a logistiky, administrátor logistiky

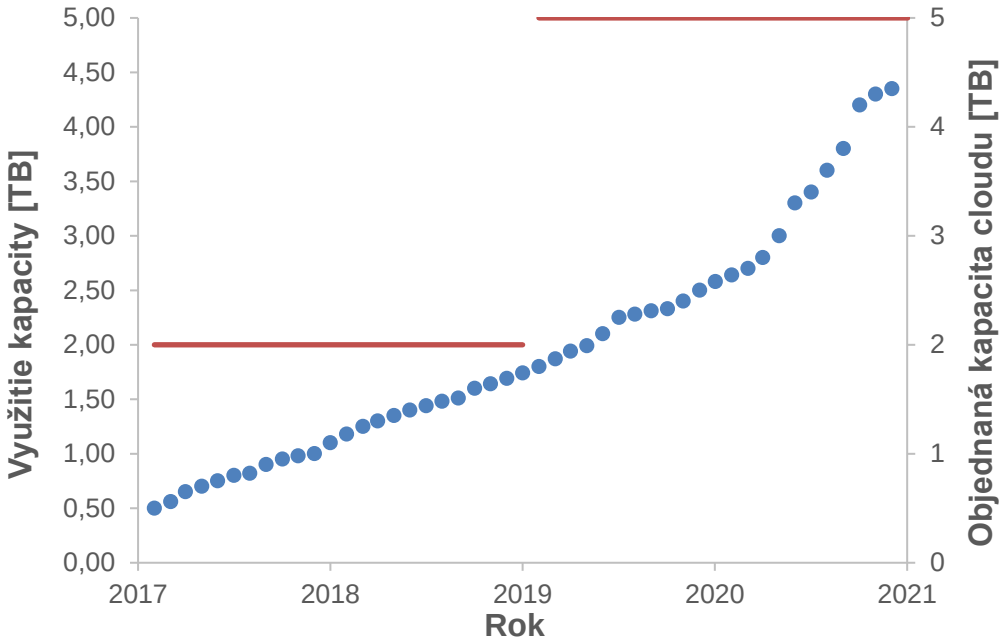
Povinnosťou každého zamestnanca je svoje dáta, ktoré sú uložené na cloude označiť správnym tagom, ktorý je určený typom dát. K dátam je automaticky pridaný aj tag vek a pôvod. Pôvod je daný poslednou osobou, ktorá dáta zmenila.

Väčšina dát je uložených na cloude, kde je vyhradená dostatočná kapacita úložiska. Všetky dáta od zákazníkov sú momentálne ukladané do cloudového priestoru a ostatné kategórie uvedené v Tab. 2.5 je možné ukladať na cloud do jeho privátnej časti. Pri týchto kategóriách môže byť prechodne pre zálohu využitý lokálny server spoločnosti aktuálne s malou kapacitou.

Nadradenou autoritou, pre administráciu dát je správca sietí, ktorý vykonáva finálne rozhodnutia o transfere dát z lokálneho úložiska a naopak a tiež má kompetenciu dáta mazať. Na vymazanie dát je však v spoločnosti nastavená krížová kontrola a správca pred vymazaním komunikuje vždy so zodpovednou osobou.

2.6 Nedostatky súčasného stavu

Doterajšie riešenie je v zásade cenovo efektívne a momentálne dostatočné, avšak pri raste spoločnosti bude potrebné využívať cloud ekonomicky efektívne, t. j. dáta, ktoré nie sú určené na aktuálne operácie alebo sú archívneho charakteru, by bolo vhodné presunúť do zabezpečeného lokálneho úložiska. Znížilo by sa tak vyťaženie cloudu a nebolo by nutné počítať s nárastom fixných nákladov na neustále zvyšovanie kapacity. Zároveň s rastom počtu zamestnancov sa zníži riziko nesprávneho nakladania s dátami, ktoré by nemali byť prístupné, t. j. zavedie sa prvok rozhodovania, kedy má byť prístup k lokálnym citlivým dátam umožnený. Na Obr. 2.1 je vidieť využívanie kapacity cloudového úložiska. Spoločnosť mala v prvých dvoch rokoch fungovania zakúpené 2 TB úložiska. K naplneniu kapacity sa spoločnosť konštantne blížila, preto musela byť kapacita v roku 2018 navýšená na 5 TB. Navýšená kapacita je dostatočná približne do roku 2021, kedy bude nutné zakúpiť vyššiu kapacitu alebo nájsť iné riešenie. Vzhľadom k prudkému nárastu využitej kapacity v poslednom roku sa javí, ako vhodné nájsť iné riešenie, ako neustále dokupovanie vyššej cloudovej kapacity.



Obr. 2.1: Graf plnenia kapacity cloudového úložiska

3 NÁVRH VLASTNÉHO RIEŠENIA

Riešenie je postavené na požiadavke lokálnej zálohy väčšieho množstva dát rôznej priority a časového rámca. Dôležitými faktormi sú kapacita, výkonnosť, bezpečnosť, škálovateľnosť, efektivita a cena. Komplexné riešenie je rozdelené do troch nezávislých funkčných blokov, ktoré tvoria výslednú systémovú reťaz vedúcu k bezpečnej zálohe dát podľa stanovených požiadaviek.

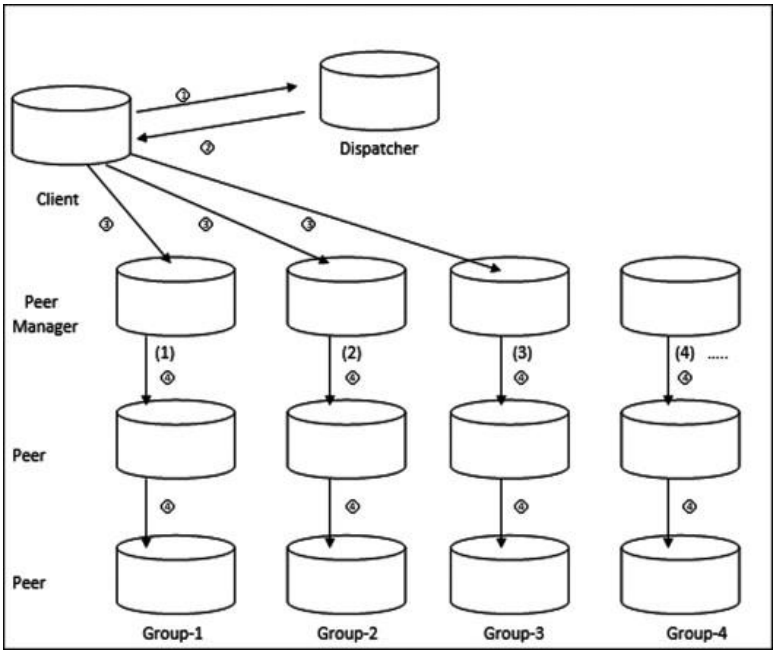
Prvým blokom riešenia je ošetrenie situácie na už využívanom cloudovom priestore, najmä privátnej časti tak, aby boli dáta v tomto priestore dostatočne analyzované – vytvorilo sa ich zaradenie na základe priority, časový rámec ich nevyhnutnej úschovy a vzniku, spôsob ďalšej manipulácie, obmedzenie prístupu k nim a tiež sa zvolili ďalšie vhodné procesy pre ich využitie. Dáta je potrebné v tejto fáze identifikovať, tzn. zvoliť do akého typu úložného priestoru dáta smerovať, kedy najskôr môžu byť dáta vymazané a či potrebné dáta dodatočne spracovávať alebo využívať. Na takúto funkciu je nutné zvoliť vhodné nastavenia prostredia a softvér, ktorý by v cloude mohol dáta týmto spôsobom triediť.

Druhý blok je tvorený vlastnou sieťovou infraštruktúrou, t. j. sieťovými prvkami uloženými a / alebo využívanými v rámci firmy, ktoré umožňujú dátový tok medzi cloudovým úložiskom a lokálnym dátovým úložiskom, prípadne v budúcnosti aj cielený tok IoT dát priamo od zákazníkov spoločnosti. Tieto prvky zahŕňajú routre, slúžiace k niekoľkonásobne zaistenému smerovaniu dát z / do cloudu (musí byť ochrana proti sieťovému výpadku napr. voľbou viacerých poskytovateľov internetu, vhodnou topológiou zariadení, monitoringom stavu zariadení a sieťových služieb). Bezpečnosť tejto infraštruktúry je zaisťovaná ochranou pomocou firewallov, ktoré majú filtrovať tok bezprostredne za / pred vstupnými / výstupnými sieťovými prvkami t. j. routrami. Okrem toho je naplánované pri úložisku vytvoriť lokálnu sieťovú infraštruktúru LAN, ktorá umožní lokálnu správu a prístup k dátam v spoločnosti a má byť tvorená prvkami miestneho charakteru, ako sú HUBy, switche, pracovné stanice a prístupové uzly. Celá sieť vystupuje ako nezávislá, ale napriek tomu sa požaduje aj autorizovaný externý prístup. Súčasťou riešenia siete sú preto aj zariadenia, ktoré poskytujú autorizáciu, zvyšujú bezpečnosť a umožňujú vzdialený prístup. Z pohľadu hardvéru ide o routre schopné nastavenie systému doménových mien (domain name system - DNS) a súkromná virtuálna sieť (virtual private network - VPN), servery, L3-switche, kde môže fungovať VPN alebo iné vhodné riešenie s pokročilou autorizáciou. Zariadenia musia byť pre spoľahlivosť duplikované ľahko nahraditeľné a zapojené tak, aby v prípade poruchy existovala alternatívna cesta pre dátový tok. Samotná konfigurácia siete je v rámci vlastného návrhu realizovaná a analyzovaná s využitím softvéru pre stavbu siete. Zvolené riešenie je tiež navrhnuté fyzicky a to so zahrnutím ekonomických faktorov s podloženými informáciami o aktuálnej trhovej situácie, čiže uskutočnením prieskumu trhu s cieľom výberu vhodných zariadení so zreteľom na ekonomickú stránku riešenia.

Tretím blokom je návrh systému vlastného úložiska. Zvolený typ architektúry úložiska reflektuje kategórie dát. Za optimálnu variantu pre dané podmienky je možné považovať úložisko typu NAS. Typ úložiska NAS je vhodný pre dáta prístupné cez programové rozhranie so známou lokáciou fyzického uloženia daných dát. Tento systém uloženia je zvolený pre dlhodobé uloženie nemenných dát, t. j. zmena alebo vymazanie takýchto dát po stanovenú dobu

neprichádza do úvahy a zároveň aj pre dáta dočasné. Na toto uloženie je použité osobitné redundantné úložisko typu RAID 6. Ďalší typ dát tvorí kategória archívnych dát, ktoré sa ukladajú do ďalších osobitných úložísk podľa hierarchie (priority) trvalo resp. na veľmi dlhú dobu. K týmto dátam sa pristupuje pomocou protokolov, je však možné ich určité využitie v procesoch. Taktiež táto časť úložiska je riešená redundantne usporiadaním v diskovom poli RAID 1.

- K vyriešeniu časti triedenia dát, distribúcie po sieti a výberu finálneho úložiska je potrebné hierarchické usporiadanie úložiska a popis systému ukladania. Infraštruktúra IoT siete vedúca ku konkrétnemu úložisku a schéma jej topológie je na Obr. 3.1. Schéma pozostáva zo štyroch zložiek: klient, dispečer, peer manažér a obyčajný peer. Klient je pôvodným vlastníkom dát (súborov). Klient kontaktuje dispečera s úmyslom získania referencie (IP adresy) konkrétneho peer manažéra (predstavuje pre klienta správcu jeho dát). Dispečer rozhoduje o priradení konkrétnej skupiny a konkrétneho peer manažéra podľa vopred definovaného kľúča pre dáta od klienta. V momente, keď sú dáta zaradené do kategórie dispečer, poskytuje klientovi cieľovú adresu peer manažéra a klient dáta odosiela. Peer manažér je správcom svojej skupiny peerov, ktorí budú predstavovať cieľové úložiská pre daný typ dát. Peer manažér rozhodne, ktorí peerovia sú vybraní na replikáciu dát, prípadne ich zdieľanie [21].



Obr. 3.1: Topológia zberu IoT dát; client – klient, dispatcher – dispečer, group – skupina [21]

Vyššie popísané rozhodovanie je už implementované v priestore cloudu a preto nie je nutné v tejto práci vyvíjať osobitný systém, tento systém má byť implementovaný až vo vzdialenejšej budúcnosti.

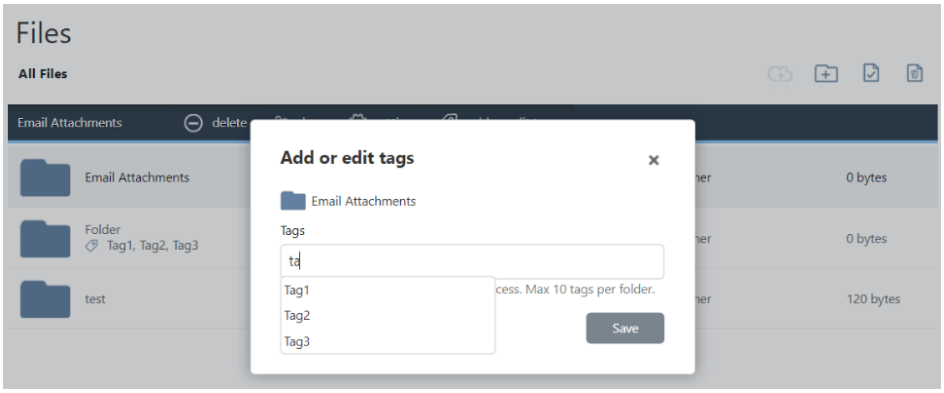
- Komplexné riešenie predstavuje samotné dátové úložisko. Pred týmto dátovým úložiskom je zaradený tzv. výpočtový modul, ktorý po prevedení dát z bloku cloudu cez sieťový blok vykonáva nad dátami rôzne operácie a bude umožnené, aby tento modul získaval aj dáta z lokálneho úložiska. Tento modul je však na úložisku aj ďalších blokoch nezávislý a nie je súčasťou riešenia uskladnenia dát.

3.1 Zmeny na cloude

Z dôvodu neustáleho nárastu objemu dát bude do spoločnosti zavedené lokálne úložisko, ktoré bude predimenzované tak, aby vystačilo aj do budúcnosti. Cloudové úložisko bude na zálohovanie aj naďalej využívané a zakúpená kapacita zostane zachovaná. Nebude už teda potrebné kapacitu cloudu zvyšovať a tak náklady na toto úložisko ostanú aj naďalej rovnaké. Prehľadnosť dát a efektivita narábania s nimi sa zvýši. Nachádzať sa tu budú iba skutočne potrebné dáta, ktoré bude navyše potrebné kategorizovať podľa nastavenej politiky. Kategorizácia dát, určenie ďalšieho využitia cloudového priestoru a spôsoby jeho zálohovania sú ďalej vysvetlené.

3.1.1 Nastavenie kategorizácie

Kategorizácia bude ďalej považovaná za povinnú súčasť pri ukladaní dát do priestoru privátneho cloudu. Postup pri kategorizácii je užívateľsky priateľský s využitím jednoduchého nástroja od Syncplicity v položke súbory – pridanie tagu (Obr. 3.2) určenej pre administrátorov, ale aj užívateľov. Všetky dáta môžu mať maximálne 10 tagov zložených z maximálne 20 znakov. V spoločnosti sa pre označovanie tagmi odporúča zaviesť nasledujúce kategórie: customers, finished_projects, projects, data_reports, management, marketing, accounting, employees, logistics. Tieto kategórie sú zavedené v súlade s politikou označovania dát podľa Tab. 2.5. Okrem toho sa nanovo zavedú logické kategórie: important (dočasne dôležité dáta), to_archive (určené k archivácii, ale s potrebou informovať správcu). Automaticky sú k dátam priradené kategórie: typ dát, veľkosť, dátum úpravy a vlastník, ktorý môže určiť ďalšie privilegované skupiny pre prácu s dátami.



Obr. 3.2: Pridávanie tagov v cloudovom nástroji Syncplicity

3.1.2 Predpokladané ďalšie využitie

Ďalšie využitie cloudu by malo spočívať najmä v operatívnom a flexibilnom využívaní dočasných projektových a iných rozpracovaných dát, prípadne dočasnom uložení dôležitých dát, pokiaľ aktuálne nie je k dispozícii možnosť uloženia v lokálnom úložisku. Naďalej bude privátny cloud využitý ako prijímací uzol pre IoT dáta od zákazníkov. Tieto však budú na cloude len krátkodobo a z cloudu budú pravidelne presmerované na lokálne úložiská. Za dátové toky a kontrolu dát existujúcich v cloude bude zodpovedný správca sietí. Verejná časť cloudu bude

naďalej využívaná doterajším spôsobom pre webové stránky a priestor pre prihlásených užívateľov, zákazníkov.

3.1.3 Zavedenie zálohy v cloudovom priestore

Na zálohovanie v cloude sa definuje nová politika záloh, striktne založená na využití obmedzenej vyčlenenej kapacity cloudového priestoru a to pre nové dáta spadajúce do vybraných kategórii: finished_projects, projects, data reports, employees, accounting a to_archive. Všetky doterajšie dáta migrujú do lokálneho úložiska a na týždennej báze bude správca vykonávať migráciu posledných IoT dát. Dáta z ostatných kategórií budú pravidelne ku koncu týždňa vymazané, s výnimkou príznaku important, ktoré umožňuje odklad jeden týždeň.

3.2 Návrh a konfigurácia siete

V rámci siete bude nastavená oblasť protokolu OSPF tak, aby bola zredukovaná veľkosť broadcastových domén, zabezpečená škálovateľnosť pri rozširovaní do ďalších priestorov a vytvorená chrbticová sieť. Jednotlivé oddelenia je vhodné logicky rozdeliť do štyroch nezávislých VLANov, pričom všetky VLAN sú zriaďované na každom z L3 switchov (redundancia). Z hľadiska požiadaviek na prípojnú kapacitu switch-ov je pre IT oddelenie, ktoré sa fyzicky nachádza v troch sekciách budovy potrebné zabezpečiť minimálne 3 switche s množstvom portov 24. Pre ostatné oddelenia je fyzicky postačujúce zabezpečiť jediný switch (t. j. pre zostávajúce oddelenia 3 kusy). Počet WiFi routrov na celkové pokrytie budovy sú dva kusy, rovnako tiež počet firewallov, ktoré budú filtrovať komunikáciu pre každú sieť pripojenú na internetového providera. Za firewallmi je potrebné zaradiť L3 switche, ktoré môžu byť súčasťou OSPF chrbticovej siete a zároveň vytvoriť VLAN na jednotlivých portoch, kde sú pripojené celé oddelenia.

Pre vývoj IT oddelenia bude zriadená serverovňa s databázovými servermi typu NAS. Komunikácia medzi VLANmi v rôznych kanceláriách bude umožnená cez L3 switch v zapojení typu Router on the Stick. V celej budove bude dostupná wifi prostredníctvom dvoch WAP (Wifi Access Points) a to routre WiFi router_1 a WiFi router_2. Prvý WiFi router_1 má pokrývať IT oddelenie a WiFi router_2 pokryje zostávajúce oddelenia. Chrbticová sieť je navrhovaná redundantne, krížovou metódou tak, aby boli všetky oddelenia pripojené k dvom nezávislým providerom. Analýza topológie, popis konfigurácie a adresovanie jednotlivých zariadení je vykonaná v kap. 3.2.2.

3.2.1 Zavedenie hardvérových prvkov

Vyhľadaním najčastejšie sa vyskytujúcich sieťových zariadení, určených pre firemné účely, bol porovnaný ponúkaný hardvér, vyrábaný renomovanými spoločnosťami pôsobiacimi v tejto oblasti. Podmienkou bol zabehnutý výrobca, dostupný servis, kvalifikácia a skúsenosti zamestnancov s daným hardvérom a jeho nastavovaním. Takýto prístup môže byť efektívny ekonomicky aj výkonnostne. Analyzované hardvérové možnosti sú uvedené v Tab. 3.1.

Tab. 3.1: Zoznam možných hardvérových prvkov pre stavbu siete [22]

Model	**Parametre**	**Cena**	**Obrázok**
Routre			
Cisco A901-12C-F-D	Pamäť typu Flash: 128 MB Kapacita pamäti: 1024 MB Priepustnosť: 1000 Mbps Porty počet + typ: 3x RJ-45, 1x SFP Spotreba energie: 40 W	2 000 €	
HPE JG409B	Pamäť typu Flash: 256 MB Kapacita pamäti: 2000 MB Priepustnosť: 1000 Mbps Porty počet + typ: 12x RJ-45, 1x SFP Spotreba energie: 300 W	2 000 €	
Switche L3			
Catalyst WS-C2960X-24TS-L	Priepustnosť: 1000 Mbps Porty počet + typ: 24x RJ-45, 4x SFP Prepínač vrstiev: L2/L3 Spotreba energie: 36,9 W	930 €	
Catalyst WS-C9260X-24PS-L	Priepustnosť: 1000 Mbps Porty počet + typ: 24x RJ-45, 4x SFP Prepínač vrstiev: L2 Spotreba energie: 49 W	1 230 €	
Switche L2			
Catalyst WS-C2960X-24TD-L	Priepustnosť: 1000 Mbps Porty počet + typ: 24x RJ-45, 2x SFP Prepínač vrstiev: L2/L3 Spotreba energie: 32,3 W	1 030 €	
Zyxel GS2220-50HP-EU0101F	Priepustnosť: 1000 Mbps Porty počet + typ: 44x RJ-45, 4x SFP Prepínač vrstiev: L2 Spotreba energie: 47,4 W	990 €	

WiFi Routre			
Cisco C891FW-A-K9	Priepustnosť: 1000 Mbps Porty počet + typ: 8x RJ-45, 1x RJ-11 Spotreba energie: 60 W	730 €	
Cisco C897VAGW-LTE-GAEK9	Priepustnosť: 1000 Mbps Porty počet + typ: 8x RJ-45 Podporuje PoE Spotreba energie: 60 W	1 000 €	
Vyrovnávač záťaže			
Cisco ASA 5508-X	Procesor: RAM: 8 GB Pamäť typu SSD: 80 GB Priepustnosť: 1000 Mbps Porty počet + typ: 8x RJ-45 Spotreba energie: 60 W	1 100 €	
Firewall			
Cisco ASA5508-K9	Pamäť typu Flash: 8000 MB Priepustnosť: 1000 Mbps Priepustnosť Firewallu: 450 Mbps Porty počet + typ: 8x RJ-45 Spotreba energie: 60 W	1 200 €	
Zyxel VPN1000-EU0101F	Priepustnosť: 1000 Mbps Priepustnosť Firewallu: 8000 Mbps Porty počet + typ: 12 RJ-45, 2x SFP Príkon/výkon: 46W	1 400 €	

3.2.2 Topológia a konfigurácia siete

V tejto kapitole sú prezentované jednotlivé sieťové celky, ktoré spolu majú tvoriť súvislú firemnú sieť spoločnosti. Navrhovaným častiam sú priradené IP adresy s podmaskami rešpektujúcimi rozsah danej siete. Pri hraničných sieťových prvkoch sú ďalej uvádzané základné konfiguračné metódy, napr. zavádzané protokoly tak, aby bol jasný účel zariadenia v celkovej hierarchii siete. IP adresovanie pre všetky sieťové celky je popísané v Tab. 3.2. Zoznam navrhovaných funkčných celkov, ktorého súčasťou sú jednotlivé oddelenia je začlenené do VLANov, je v Tab. 3.3. Funkčné celky sú ohraničené logicky podľa príslušnosti k oddeleniam, fyzického umiestnenia v rámci firmy a distribúcie kapacity úložiska do dotknutých častí firmy. Do funkčných celkov sa zaraďuje chrbticová sieť, čo je najdôležitejšia štruktúra slúžiaca ku pripojeniu periférnych logicky definovaných firemných podsietí. Medzi periférie patria podsiete, do ktorých sú začlenené jednotlivé oddelenia: IT, HR a marketing, obchod a logistika. V samostatnom podsystéme sú zavedené dve nezávislé dátové úložiská:

- Prvé pre IT oddelenie a zálohu IoT dát tvorené NAS servermi.
- Druhý podsystém má slúžiť na archiváciu dokumentov pre ostatné oddelenia a tvoriť ho bude archivačný server.

Súčasťou návrhu chrbticovej siete je zavedenie vlastnej autonómnej oblasti vo firme pomocou OSPF protokolu, ktorý umožní škálovateľnosť, obsluhu siete pri výpadkoch a poruchách zariadení a bude podávať informácie o všetkých zmenách na jednotlivých sieťových prvkoch v tejto oblasti. Do OSPF oblasti je vhodné zaradiť kľúčovú chrbticovú sieť spoločnosti bez priľahlých periférii a podsietí dátových úložísk, aby sa predišlo zväčšovaniu veľkosti broadcastových domén a zvýšila sa rýchlosť a efektivita práce tejto najdôležitejšej sieťovej štruktúry. V OSPF oblasti definovanej ako OSPF Area 1 sa nachádzajú ako hraničné prvky ISP prístupové routre a L3 switche. Medzi nimi sú v oblasti Area 1 firewally, filtrujúce komunikáciu prichádzajúcu alebo odchádzajúcu z alebo do internetu.

Na perifériách a v častiach dátových úložísk sú podľa príslušnosti k danému oddeleniu alebo úložisku zriadené VLAN. Toto riešenie umožňuje zmenšiť rozsah pripojovaných zariadení a ich údržbu v menších sieťových celkoch. Prehľad navrhovaných VLANov je uvedený v Tab. 3.3.

Prípad pripájania firemných zariadení z prostredia internetu do lokálnej firemnej siete je riešený pripojením pomocou virtuálnej súkromnej siete (VPN). Na ISP prístupových routroch je pre tento účel zavedený protokol IPSec, pomocou ktorého je vytvorený tunelový typ virtuálneho pripojenia k lokálnym zdrojom cez internet. V rámci tohto protokolu je ako najvhodnejšie riešenie implementovaný protokol ESP (Encapsulation Security Payload). Pre tento protokol sú na routroch nastavený peerovia (hostiteľské zariadenia), využívajúci zabezpečené tunelové pripojenie z internetu do firemnej siete. Vzhľadom k veľkosti firmy a malému počtu koncových užívateľov (prístupových bodov) sú z dôvodu bezpečnosti zadané šifrovacie a overovacie kľúče (IK, Internet Keys Exchange) s protokolom IPSec zadávané pre VPN manuálne, tzv. manuálne kľúčovanie.

- Prístupové routre: navrhuje sa zavedenie VPN, DNS, OSPF a BGP protokolov a využitie interného firewallu pre filtrovanie paketov.
- L3 switche majú zavedený protokol OSPF.
- WiFi routre majú zavedené protokol OSPF a taktiež protokol DHCP.
- Na Switche jednotlivých oddelení sú konfigurované VLANy.

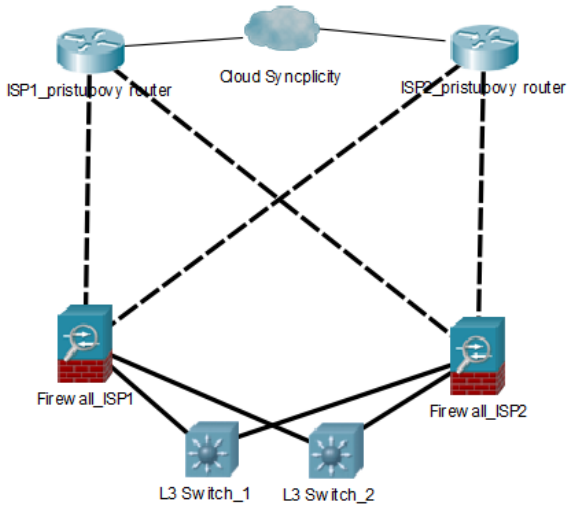
Tab. 3.2: IP adresovanie navrhovaných sieťových prvkov spojených s lokálnym úložiskom

Zariadenie	IP adresa typ	IP adresa siete	Podmaska
ISP1_pristupovy router	OSPF paterni oblasť	172.1.1.0	255.255.255.240
	Internet provider 1	90.108.10.12	255.255.0.0
ISP2_pristupovy router	OSPF paterni oblasť	172.1.2.1	255.255.255.240
	Internet provider 2	95.86.150.32	255.255.0.0
L3 switch_1	OSPF	172.1.1.0	255.255.255.240
	VLAN 10 (IT)	10.10.10.0	255.255.255.0
	VLAN 20 (HR a marketing) marketing)	20.20.20.0	255.255.255.0
	VLAN 30 (Obchod)	30.30.30.0	255.255.255.0
	VLAN 40 (Logistika)	40.40.40.0	255.255.255.0
	VLAN 101 (Storage1)	101.101.101.0	255.255.255.240
	VLAN 102 (Storage2)	102.102.102.0	255.255.255.240
L3 switch_2	OSPF	172.1.1.0	255.255.255.240
	VLAN 10 (IT)	10.10.10.0	255.255.255.0
	VLAN 20 (HR a marketing) marketing)	20.20.20.0	255.255.255.0
	VLAN 30 (Obchod)	30.30.30.0	255.255.255.0
	VLAN 40 (Logistika)	40.40.40.0	255.255.255.0
	VLAN 201 (Archive)	201.201.201.0	255.255.255.240
WiFi router_1	OSPF	172.1.1.0	255.255.255.240
	WiFi 1	192.168.1.0	255.255.255.0
WiFi router_2	OSPF	172.1.1.0	255.255.255.240
	WiFi 2	192.168.2.0	255.255.255.0

Tab. 3.3: Zoznam switchov priradených do navrhovaných VLAN sietí

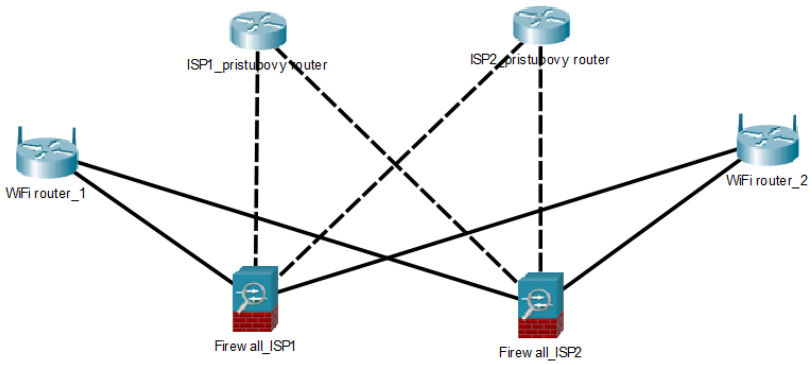
VLAN	Zoznam Zariadení
VLAN 10 – IT oddelenie (10.10.10.0)	IT Switch_1
	IT Switch_2
	IT Switch_3
VLAN 20 – HR a marketing (20.20.20.0)	HR+marketing switch_1
VLAN 30 – Obchod (30.30.30.0)	Obchod Switch_1
VLAN 40 – Logistika (40.40.40.0)	Logistika Switch_1
VLAN 101 (Storage1) 101.101.101.0	IoT line NASserver_1
	IoT line NASserver_2
	IoT line NASserver_3
VLAN 102 (Storage2) 102.102.102.0	IoT line NASserver_4
	IoT line NASserver_5
VLAN 201 (Archive) 201.201.201.0	Archive Server

Štruktúra chrbticovej siete (zobrazená na Obr. 3.3) je vystavaná tak, aby bola zabezpečená redundancia internetového pripojenia dvomi nezávislými internetovými providermi. Routre, ktoré sú priamo pripojené k sieťam poskytovateľov, sú označené ako ISP prístupový router. Na týchto routroch je zriadený protokol BGP, zabezpečujúci komunikáciu smerom do internetu a teda aj na cloudové úložisko spoločnosti. Na routroch je tiež zavedený protokol OSPF, ktorý vytvára jednoduchú vlastnú doménu v spoločnosti. Za routrami sú z bezpečnostných dôvodov umiestnené firewally, filtrujúce komunikáciu z a do internetu. Na firewally sú napojené L3 switche, ktoré vytvárajú lokálne pripojenia ku zvoleným VLAN sieťam a k sieti dátového úložiska. L3 switche sú navrhované pre podporu protokolu OSPF (spoločne s routrami fungujú ako tzv. hraničné routre oblasti OSPF). V prípade nutnosti môžu tiež smerovať komunikáciu smerom na internet namiesto routrov.



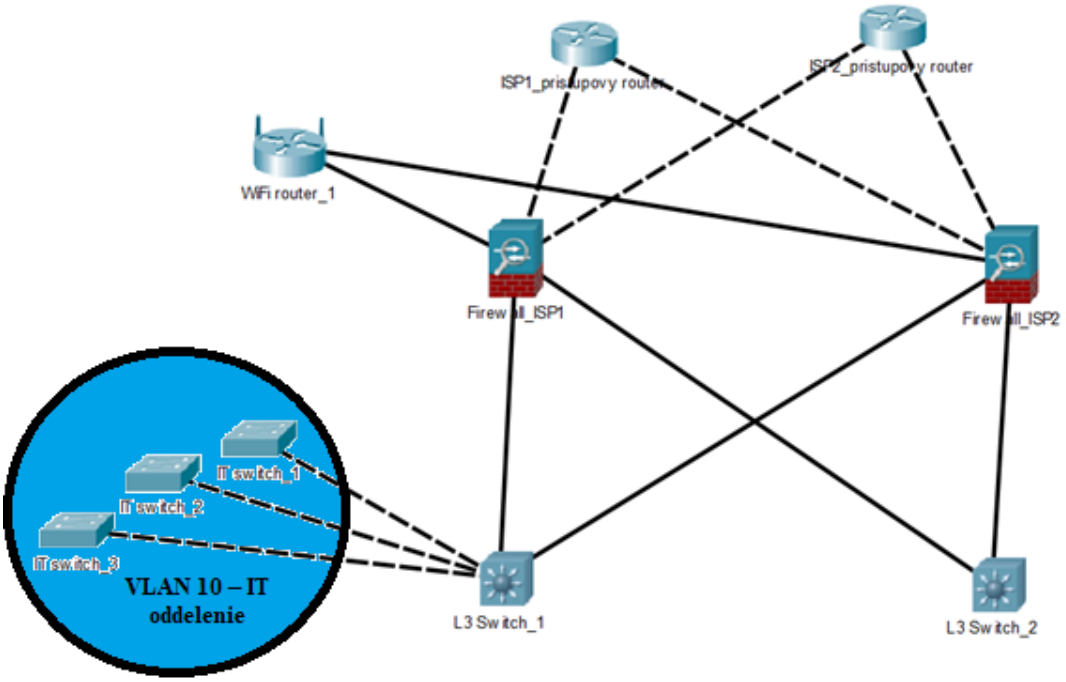
Obr. 3.3: Chrbticová sieť

Na Obr. 3.4 je zobrazená jednoduchá schéma firemnej WiFi siete, kde sú k zariadeniam chrbticovej siete pripojené dva WiFi routre, ktoré svojím výkonom pokrývajú potreby distribúcie bezdrôtovej komunikácie. Na routroch sa bude vyžadovať autentifikácia pre prístup do WiFi siete. Možnosť prístupu bude filtrovaná MAC adresami s obmedzeným počtom zariadení.



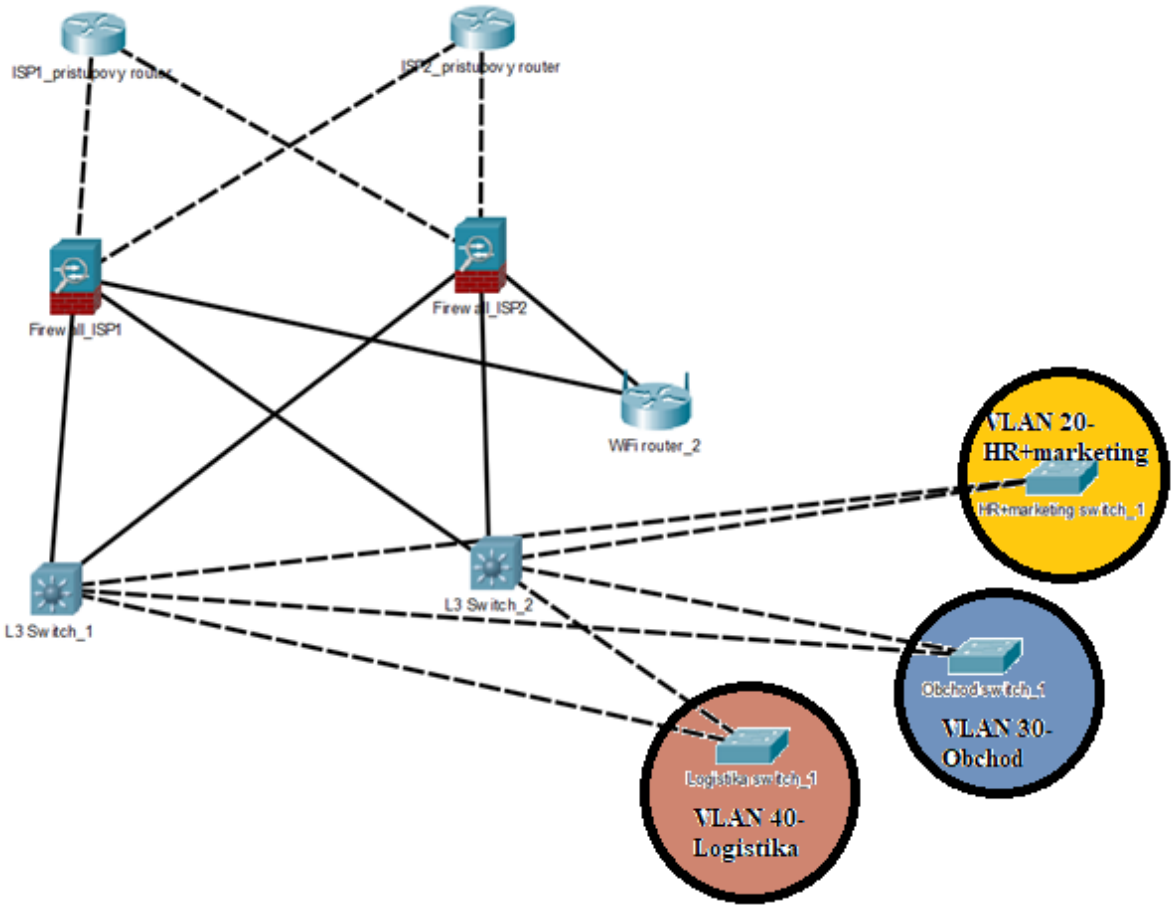
Obr. 3.4: WiFi sieť

Lokálna sieť označená ako periféria IT (zobrazená na Obr. 3.5) zahŕňa tri switche prevádzkované oddelením IT, rozmiestneným v troch častiach budovy. V tejto sieti je na switchoch nakonfigurovaná VLAN 10, projektovaná pre pokrytie potrieb IT oddelenia. Spojenie medzi switchmi IT oddelenia a L3 switchom_1 chrbticovej siete je typu Trunk (distribuujú sa pakety všetkých VLANov).



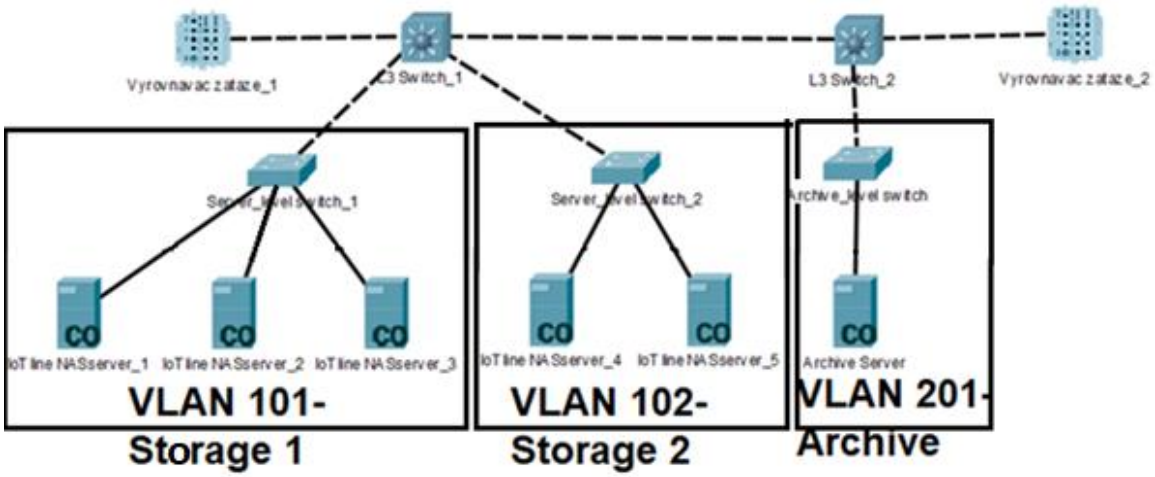
Obr. 3.5: Periféria IT

Lokálne siete tvoriace periférie oddelení HR a marketing (VLAN 20), obchodného oddelenia (VLAN 30) a oddelenia logistiky (VLAN 40) sú zobrazené na Obr. 3.6. Na každé oddelenie postačuje jeden vlastný switch. Switche jednotlivých oddelení sú konfigurované do príslušnej lokálnej VLAN podľa Obr. 3.6. Pre tieto oddelenia je zabezpečená duplicita pripojenia prostredníctvom zavedenej komunikácie s obidvoma L3 switchmi. Komunikácia medzi switchmi oddelení a L3 switchmi je typu Trunk. L3 switch_1 je nakonfigurovaný tak, aby filtroval komunikáciu smerom k pripojenému dátovému úložisku pre všetky oddelenia s výnimkou IT, t. j. jediný prístup k tomuto úložisku má IT oddelenie.



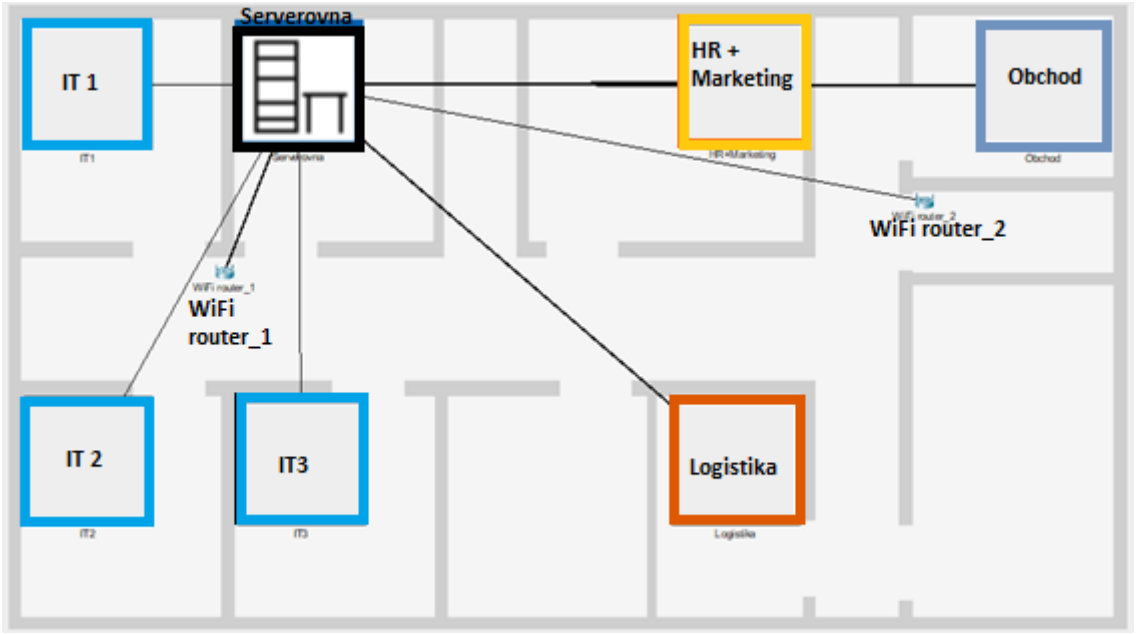
Obr. 3.6: Periféria HR a marketing, obchodné oddelenie a logistické oddelenie

Sieťová časť lokálneho dátového úložiska je schematicky zobrazená na Obr. 3.7. Sieťová časť úložiska je rozdelená na dva celky od úrovne L3 Switchov. L3 Switch_1 je nadradeným prvkom pre smerovanie dát do IoT časti úložiska. Táto časť úložiska je vyhradená pre IT oddelenie a je tvorená piatimi NAS servermi a dvoma switchmi nad úrovňou serverov pre pripojenie a rozdeľovanie toku dát na príslušný server. Druhá časť úložiska je určená pre archiváciu dokumentov zostávajúcich oddelení spoločnosti. Tvorí ju jeden archivačný server (využije sa pôvodný NAS server, ktorým spoločnosť už disponuje) a jeden switch nad úrovňou servera. Okrem týchto prvkov sú na kritických miestach tejto siete, t. j. L3 switchoch zapojené zariadenia pre vyrovnávanie sieťovej záťaže. Táto sieť nebude súčasťou oblasti OSPF, aby sa predišlo zväčšovaniu veľkosti broadcastovej domény. Medzi L3 switchmi a servermi je zaradená vrstva switchov, na ktorých sú definované vlastné VLAN podsiete. Takto je zabezpečené logické delenie úložiska a škálovateľnosť logických celkov úložiska, s možnosťou pripojiť ďalšie zariadenia k daným switchom. Na efektívne fungovanie sa predpokladá zapojenie maximálne piatich NAS serverov na jeden switch.



Obr. 3.7: Sieťová časť dátového úložiska

Približné fyzické rozmiestnenie sieťovej infraštruktúry v spoločnosti je vo forme pôdorysu zobrazenej na Obr. 3.8. Pôdorys je výstupom programu Packet Tracer a na jeho základe je približne možné určiť predpokladané dĺžky kabeláže a potrebného rozmiestnenia sieťových zdrojov.



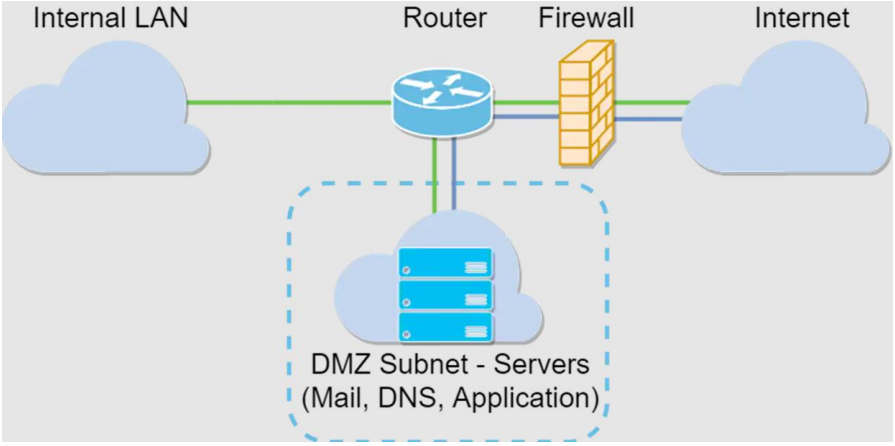
Obr. 3.8: Pôdorys sieťovej infraštruktúry spoločnosti

3.2.3 Zaistenie bezpečnosti siete

Bezpečnosť vlastnej firemnej siete závisí predovšetkým na správnej konfigurácii bezpečnostných prvkov – firewallov. Na firewalloch je potrebné zaviesť filtrovanie paketov tak, aby pre hostiteľov z lokálnej firemnej siete bolo možné dosiahnuť akýkoľvek externý zdroj,

nachádzajúci sa na internete a zároveň bolo obtiažne pre hostiteľov z prostredia internetu dosiahnuť prístup do lokálnej firemnej siete. Riešením môže byť zavedenie stavového paketového filtrovania na obidvoch firewalloch. Na tento účel možno využiť filtrovanie s príznakom bitu ACK, napr. tak, že tento príznak bude mať pre pakety pôvodom z lokálnej siete a príslušného portu hodnotu nula. Naopak bitový príznak ACK pre pakety prichádzajúce z internetu a príslušného portu bude mať hodnotu jedna. Týmto spôsobom sa zvýši aj ochrana pred útokmi typu DoS. Táto úroveň ochrany môže byť dostatočná pre zariadenia lokálnej siete, ale pre dátové úložisko je vhodné aplikovať dodatočnú ochranu konfiguráciou demilitarizovanej zóny (DMZ). Ide o fyzickú alebo logickú podsieť, ktorá oddeľuje internú LAN od iných nedôveryhodných sietí, zvyčajne verejného internetu. Z internetu sú dostupné iba prístupové routre a zvyšok siete ostáva nedosiahnuteľný pre prístup nepovoleným užívateľom. V prípade, že útočník napadne lokálnu sieť, budú NAS servery lokálneho úložiska mimo jeho dosahu. DMZ je navrhovaná podľa odporúčaní spoločnosti Cisco v topológii DMZ podsiete uvedenej na Obr. 3.9. V tejto topológii ležia ostatné zariadenie lokálnej siete mimo DMZ a na firewalle je DMZ nastavená zaradením sietí s príslušnými maskami (VLANy dátového úložiska) do zoznamu chránených. Spoločne so zriadeným DMZ môžu byť na firewalle aktivované systémy detekcie prieniku. V návrhu sa počíta so zriadením DMZ pomocou jedného firewallu. Komplexné riešenie siete umožňuje v prípade požiadaviek, daných firemnou politikou, pripojiť na vstupné routre (pred detekciu firewallom), zaradiť verejne prístupné sieťové prvky, ako napr. webový server a iné zariadenia, ktoré budú ležať mimo chránenú oblasť lokálnej siete. Tieto je možné chrániť interným firewallom, ktorý je súčasťou navhrnovaných vstupných routrov. Tieto zariadenia nie sú súčasťou riešenia vlastného dátového úložiska a ochrany lokálnej siete, preto nie sú v práci uvádzané. Každý takýto zriadený server by pri navrhovanej sieťovej štruktúre umožňoval v kombinácii s interným firewallom vstupného routra zavedenie aplikačnej brány. Ide o server kontrétnej aplikácie, ktorý umožňuje prechod všetkých dát danej aplikácie s nastavením vybraného portu. Zvolené prístupové routre umožňujú taktiež zriadenie tunelovej VPN pre prístup zamestnancov z externých zdrojov z prostredia internetu a súčasne konfiguráciu routra ako prístupového DNS servera. Konkrétne nastavenia jednotlivých zariadení siete majú sledovať predkladanú filozofiu sieťovej infraštruktúry [23–25].

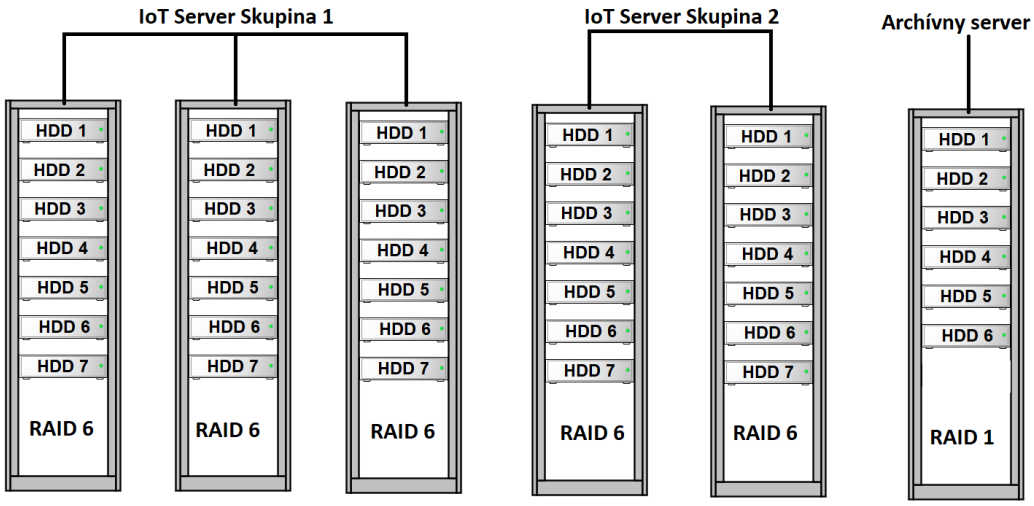
Osobitne je potreba pristupovať k efektívnej a bezpečnej konfigurácii lokálnej siete. Na zvýšenie efektivity sa v rámci chrbticovej siete navrhuje zaviesť oblasť protokolu OSPF, ktorá nebude z hľadiska počtu zariadení tvoriť príliš veľkú broadcastovú doménu. OSPF zabezpečí efektívne a bezpečné pripájanie prípadných nových pripájacích zariadení. V perifériách budú pre efektivitu a bezpečnosť, pre potreby jednotlivých oddelení a dátového úložiska zriadené VLANy, ktoré umožnia využitie siete v menších jednotkách bez sieťových konfliktov, napr. zdieľanie tlačiarne pre určité oddelenie. Lokálna WiFi sieť konfigurovaná na dvoch WiFi routroch (prideľovanie protokolom DHCP) bude pre prístup vyžadovať autorizáciu so šifrovaným kľúčom WPA2 – Enterprise a zariadenia budú filtrované napríklad na základe MAC adries [23,25].



Obr. 3.9: Navrhovaná topológia DMZ zóny; subnet -podsieť, servers – servery, application – aplikácia, internal - vnútorná [23]

3.3 Návrh vlastného lokálneho úložiska

Z dôvodu rozdielnych objemov dát je adekvátnym riešením rozdelenie plánovanej kapacity lokálneho úložiska na dve časti. Prvá časť je dimenzovaná na vysokú kapacitu pre zálohovanie veľkých objemov IoT dát a z hľadiska organizácie má prislúchať výlučne IT oddeleniu. Túto časť je možné zložiť z niekoľkých paralelných NAS serverov tak, aby bola rešpektovaná štruktúra ukladania IoT dát podľa schémy na Obr. 3.1. Presný počet týchto serverov je 5, pričom, na každom NAS serveri je plánovaných 7 diskov. Druhá časť lokálneho úložiska má slúžiť pre dedikovaný archivačný server, určený pre archiváciu dokumentov. Na tento účel bude postačovať jeden server typu NAS so šiestimi diskami. V obidvoch prípadoch sú vzhľadom na cenu, kapacitu, spoľahlivosť a možný počet zápisov zvolené fyzické disky s magnetickým zápisom HDD.



Obr. 3.10: Návrh usporiadania lokálneho úložiska

3.3.1 Výber nového hardvéru

Na základe komplexnosti ponúkaných riešení vychádza ako vhodná voľba server SynologyDS2419+, ktorý ponúka podporu pre 12 diskových jednotiek. Je modulárny z pohľadu hardvérového vybavenia, možno na ňom zaviesť softvérové radiče. Škálovateľnosť umožňuje doplnenie až na 24 diskových jednotiek. Sieťové karty a pamäť RAM sú taktiež modulárne. Za diskové jednotky je optimálne zvoliť HDD WD Gold s kapacitou 10 TB. Táto kombinácia je efektívna z pohľadu ceny a postačujúca pre danú aplikáciu.

Tab. 3.4: Výber dostupných hardvérových prvkov [26]

Model	**Parametre**	**Cena**	**Obrázok**
Diskové úložiská			
HDD WD Gold 10 TB	Rýchlosť čítania: 262 MB/s Rýchlosť zápisu: 262 MB/s Cache: 256 MB Otáčok za minútu: 7 200 Kapacita: 10 TB Spotreba: 9,2 W	280 €	
WD Gold SSD 7.68 TB	Rýchlosť čítania: 3 100 MB/s Rýchlosť zápisu: 1 800 MB/s Cache: 256 MB Kapacita: 7.68 TB Spotreba: 12 W	1 800 €	
Server NAS			
Asustor AS – 7008T	Kapacita: 8x SSD + HDD Procesor: Intel Core i3 3,5 GHz RAM: 2048 MB DDR3 Rozhranie: 3x USB 3.0, 2x USB 2.0, 2x LAN, 2x eSATA Podporovaný RAID: 0, 1, 5, 6, 10 Spotreba: 80 W	1 400 €	
Synology DS2419+	Kapacita: 12x SSD + HDD Procesor: Intel Atom C3538 2,1 GHz RAM: 4096 MB DDR4 Rozhranie: 4x LAN, 2x USB 3.0 Podporovaný RAID: 0, 1, 5, 6, 10 Spotreba: 101,6 W	1 600 €	

UPS zdroje			
APC Back-UPS BX 700	Skutočný výkon: 390 W Hmotnosť: 6 kg Záložná doba pri 100% záťaži: 1 min Záložná doba pri 50% záťaži: 8 min Zásuvky: 3x FR Dodatočné rozhranie a ochrana: USB	100 €	
APC Back-UPS BX 1400	Skutočný výkon: 700 W Hmotnosť: 12 kg Záložná doba pri 100% záťaži: 1 min Záložná doba pri 50% záťaži: 8 min Zásuvky: 4x FR Dodatočné rozhranie a ochrana: ochrana telefónnej siete RJ-11, USB	160 €	
APC Smart-UPS 2200 VA LCD 230 V	Skutočný výkon: 1 980 W Hmotnosť: 48,8 kg Záložná doba pri 100% záťaži: 8,7 min Záložná doba pri 50% záťaži: 25 min Zásuvky: 8x IEC 320 C13, 1x IEC 320 C19, 2x IEC Jumpers Dodatočné rozhranie a ochrana: USB, Ethernet	1 000 €	

3.3.2 Usporiadanie v diskových poliach a nastavenie

Schéma vlastného úložiska je na Obr. 3.10. V schéme sú z dôvodu údržby a škálovateľnosti vytvorené uzly pozostávajúce z rovnakých HDD. Zlyhanie každého z týchto uzlov by mohlo mať závažné dôsledky pre ochranu dát. Koncept úložiska rešpektuje kapacitné potreby IT oddelenia pre ukladanie IoT dát a archiváciu dokumentov pre ostatné oddelenia. Riešením je rozdelenie toku dát na dve časti, dáta smerujúce na jediný archivačný server – dlhodobo zálohované dáta menšieho objemu, ktoré nie sú typu IoT (napr. zmluvy, technické riešenia, projekty, a pod.) a niekoľko serverov NAS pre zálohu IoT dát. Prvú časť úložiska tvorí päť nezávislých NAS serverov. Druhá časť úložiska je tvorená jedným archívnym NAS serverom, pre zálohovanie dokumentov. Ak zvažujeme dodatočnú ochranu IoT dát (prvá časť úložiska) viacnásobným zálohovaním, je nutné v týchto uzloch vytvoriť redundantné pole nezávislých diskov RAID. Z bezpečnostných dôvodov sa aplikácia RAID 6 javí, ako vhodné

riešenie okamžitej obnovy dát, po zlyhaní ľubovoľných dvoch diskov. Archivačný server je možné zálohovať spôsobom zrkadlenia podľa typu diskového poľa RAID1. Na archivačnom serveri sa diskové pole rozdelí na 2 série identických diskov. Na začiatku budú postačovať 3 disky, na sériu celkovo teda 6.

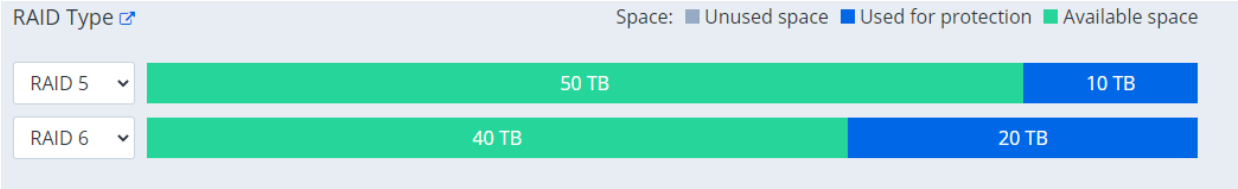
Pole RAID 6

Diskové pole RAID 6 bude, z už diskutovaných dôvodov, ako je zvýšená ochrana dát a možnosť zefektívnenia procesov zápisu a čítania, zvolené pre päť nezávislých uzlov (päť NAS serverov) IoT úložiska. V jednom uzle (NAS serveri) je uložených sedem rovnakých HDD diskov kapacity 10 TB. Ďalšie riešenie predpokladá, že HDD nie je opraviteľná komponenta systému. Preto siedmy disk je vyčlenený na disky typu tzv. „spare“, t. j. disky v pohotovosti navyše, ktoré okamžite nahrádzajú poškodený disk. V kap. 3.5 bude preto diskutovaná politika údržby a okamžitej výmeny HDD pri zlyhaní. Počet diskov a celková kapacita úložiska v jednom uzle bola stanovená na základe diskutovaných odporúčaní a vlastností RAID 6. Diskové pole musí mať v tomto prípade najmenej štyri disky, zvyšovaním počtu diskov rastie efektivita vzhľadom ku kapacite, na zvýšenie stupňa ochrany je vhodné zaradiť spare disk. Avšak vysoký počet diskov zvyšuje pravdepodobnosť zlyhania disku alebo súčasného zlyhania diskov, zároveň zvyšuje náklady na energie, údržbu a hardvér diskového radiča. Stredná doba do zlyhania diskového poľa (*MTTF*) je nepriamo úmerná počtu diskov, platí vzťah [27]:

$$MTTF = \frac{t_f}{D} \qquad (1)$$

kde t_f je priemerný čas, za ktorý zlyhá jeden disk a D je počet diskov v poli. Zo vzťahu (1) je zrejmé, že v akomkoľvek prípade pri raste počtu rovnakých diskov sa stredná doba do zlyhania diskového poľa skracuje.

Na výpočet kapacity navrhovaného riešenia bola využitá online RAID 6 kalkulačka od spoločnosti Synology (navrhovaný dodávateľ NAS serverov). Výpočet pre uvažovaných 6 HDD diskov kapacity 10 TB v porovnaní diskových polí RAID 5 a RAID 6 je na Obr. 3.11 [28]. Z výpočtu vyplýva, že na ochranu je vyčlenených 20 TB a na ukladanie dát zostáva k dispozícii 40 TB (predstavuje 66,7 %) celkovej kapacity jedného uzlu. Pri použití RAID 5 usporiadania, by bolo možné využiť až 50 TB (83,3 %) z celkovej kapacity uzlu, ale za cenu zníženia ochrany dát. Súhrnná kapacita všetkých uzlov diskového poľa RAID 6 je 200 TB.



Obr. 3.11: Výpočet kapacity pri riešení úložiska pomocou RAID 6 [28]

Relatívne nízka sekvenčná rýchlosť zápisu / čítania: 671 MB/s / 1716MB/s (pre Synology DS2419+ a danej technickej špecifikácii) môže byť hardvérovo akcelerovaná. Akcelerácia je možná vďaka modulárnemu hardvéru, ktorý môže byť doplnený o nové prvky. Možná je aj softvérová akcelerácia, preto sa navrhuje OS na báze Linux, ktorý bude účelne využitý len pre

potreby radiča RAID 6. Všetky hardvérové a softvérové zmeny, ktorých cieľom má byť akcelerácia dátového úložiska je potrebné vyhodnocovať z hľadiska výkonu a stability pomocou benchmarku. V zásade je dobré stanoviť politiku kontroly každej v budúcnosti navrhovanej zmeny a kvantitatívne ju vyhodnotiť benchmarkom funkčným v prostredí Linux / Unix. Ako použiteľný príklad možno uviesť benchmark Bonnie++ [27].

Pole RAID 1

Pre archiváciu sa zavádza usporiadanie diskového poľa RAID 1, kde bude použitý už zabehnutý NAS server DELL PowerEdge R740, vybavený šiestimi 10 TB HDD diskami. Server NAS bude ďalej slúžiť ako archívny a vzhľadom k aplikovanému RAIDu bude disponovať kapacitou 30 TB, zvyšných 30 TB bude zrkadlených pre zálohu dát.

3.4 Zhodnotenie navrhovaného riešenia

V celkovom hodnotení navrhovaného riešenia sa analyzujú výhody a nevýhody technického riešenia a hlavné body technickej stránky. Investičné a prevádzkové náklady navrhovaného riešenia sú v jednoduchej analýze uvedené v podkapitole 3.4.2.

3.4.1 Analýza technickej stránky zvoleného riešenia

Výhodou predkladaného riešenia je zachovanie doterajšieho stavu cloudového úložiska, ktoré bude naďalej k dispozícii pri zachovaní jeho kapacity. Väčšia časť kapacity bude po zavedení lokálneho úložiska dostupná pre krátkodobú prácu, čím sa pre zamestnancov spoločnosti zvýši efektivita využitia cloudu. Zámerne sa v riešení neuvažujú veľké zásahy, ale odporúča sa len implementácia potrebných nastavení a zavedenie bezpečnostných politík. Po týchto drobných zásahoch možno považovať cloudový priestor za optimalizovaný. Nevýhodou je, že podstatná časť bezpečnosti cloudu bude stále závisieť na ľudskom faktore.

Architektúra sieťovej infraštruktúry je navrhovaná s uplatnením zásad škálovateľnosti, bezpečnosti, redundantného pripojenia, výkonnosti a možnosti organizácie do menších celkov. Škálovateľnosť je zaistená od úrovne chrbticovej siete, kde je aplikovaný OSPF protokol. Chrbticová sieť je schopná okamžite reagovať na zmeny v sieti, či už z dôvodu poruchy alebo pridania nového zariadenia. Škálovateľnosť menších sieťových celkov – periférii je zaistená podsieťami typu VLAN, ktoré sú adresované IP adresami s dostatočným rozsahom pre pripájanie zariadení k switchom. Switche boli vybrané tak, aby disponovali dostatočným počtom portov pre pripojenie zariadení. Požiadavka škálovateľnosti je uplatnená aj v časti siete pre dátové úložisko, kde je možné zavádzať niekoľkonásobne väčšie množstvo serverových jednotiek, ako tomu je v aktuálnom návrhu. Bezpečnosť je riešená už od vstupných zariadení, ktoré tvoria výkonné routre s integrovaným firewallom, ktoré v budúcnosti umožnia vytvoriť externe prístupnú sieť spoločnosti nad úrovňou filtrovania samostatným firewallom. Na vstupných routroch sú aplikované užitočné služby, sprostredkované protokolmi VPN a DNS, ktoré sú bezpečnostnými prvkami pre pripojenie pracovníkov z externej siete. Nižšie funkčné celky (periférie a úložisko) sú zahrnuté z dôvodu bezpečnosti a predchádzania konfliktom medzi zariadeniami do VLAN podsietí. Nad lokálnou sieťou sú zaradené výkonné bezpečnostné prvky – firewally, na ktorých je využitá možnosť filtrovania dátových tokov, systémy detekcie prieniku a vytvorená DMZ, ktorá obsahuje lokálne dátové úložisko. Bezpečnostné riešenie je pomerne zložité, náročné na správu a hardvér. Jeho výhodou však je

značná eliminácia ľudského faktoru s využitím súčasných možností sieťového zabezpečenia. Sieť je koncipovaná redundantne, čo je zaistené dvoma nezávislými poskytovateľmi siete, ku ktorým sa spoločnosť pripája cez dva vstupné routre. Chrbticová sieť je navrhnutá spôsobom umožňujúcim okamžitú reakciu na stratu jedného z pripojení do internetu a to pre všetky nižšie sieťové celky (akákoľvek periféria má k dispozícii pripojenie od obidvoch poskytovateľov). Výkonnosť siete je ovplyvnená najmä voľbou predimenzovaného hardvéru, v chrbticovej sieti sa uplatňuje zásada minimálne gigabitového prenosu medzi portami zariadení, s možnosťou zoskupovania portov do väčších skupín, pre zvýšenie priepustnosti dát (napr. ether channel). Kritickým bodom je sieť dátového úložiska, kde okrem použitia výkonných vstupných L3 switchov, sú na týchto pripojené aj vyrovnávače záťaže. Vyrovnávače záťaže slúžia na kompenzáciu výkonu v prípade špičiek dátových tokov. Nevýhodou opäť budú nároky na hardvér a údržbu, ale priorita dostatočných sieťových zdrojov je týmto naplnená. Menšie sieťové celky sú vytvárané na zariadeniach nižšej úrovne, priamo pripojených k chrbticovej sieti. Na organizáciu a správu týchto celkov sú vytvorené VLANy.

Dátové úložisko pozostáva z dvoch častí NAS serverov, pre ukladanie a zálohu IoT dát a archívneho serveru. Z hľadiska využitia a kapacity sú tieto dve časti rozdielne. Preto sa pri návrhu redundantného úložiska zaviedli dva rôzne typy diskových polí RAID. Pre väčšiu časť, t. j. úložisko IoT dát rozhodovalo medzi RAID 5 a RAID 6. Tieto diskové polia sú odporúčané ako cenovo efektívna voľba pre malé a stredné podniky [29].

RAID 5 poskytuje ochranu dát aj pri zlyhaní jedného disku, pričom využíva distribuované paritné informácie na všetkých diskoch poľa. Pole RAID 5 v porovnaní s RAID 6 je flexibilnejšie z pohľadu čítania dát, zápis je však pomalší. Významným dôvodom v prospech zavedenia RAID 6 je však schopnosť obnovy dát, aj v prípade chyby čítania, pri prestavbe diskového poľa po zlyhaní disku. Chyba v čítaní pri prestavbe poľa po zlyhaní disku v prípade RAID 5 je nezvrátiteľná (nie je k dispozícii ďalší kontrolný súčet) a dochádza k strate dát. RAID 6 je schopný pri zlyhaní jedného disku takéto dáta obnoviť. Oproti RAID 5 je možné obnoviť dáta prestavbou aj pri zlyhaní dvoch diskov (tu však už nesmie nastať chyba pri čítaní dát). V návrhu je uvažované vysokokapacitné pole s viacerými diskami, určené pre kriticky dôležité dáta, kde sa na pravdepodobnosť zlyhania nahliada konzervatívne a zlyhanie minimálne jedného disku je považované za častý jav a chyby čítania pri obnove poľa za dosť pravdepodobné. Z dôvodu vyššej ochrany sa ako výhodnejšie riešenie pre túto časť dátového úložiska navrhuje zavedenie diskového poľa RAID 6. Nevýhoda spojená s nižšími rýchlosťami zápisu, ale najmä čítania, sa odporúča riešiť hardvérovou a softvérovou akceleráciou, po dôkladnej analýze dátových tokov a výkonu vo fáze testovania s využitím benchmarku. S týmto riešením je samozrejme spojená nutnosť dodatočných nákladov pri optimalizácii úložiska za chodu. Ďalšou nevýhodou zvoleného prístupu je zložitosť ovládača, nutnosť použitia diskov navyše pri znížení využiteľnej kapacity na úkor ochrany. Na dodatočnú ochranu sa navyše odporúča zaviesť pohotovostný disk (spare disk) pre okamžitú náhradu poškodeného disku. Celková využiteľná kapacita v piatich nezávislých NAS serveroch po zavedení RAID 6 bola dimenzovaná až na 200 TB. NAS servery sú volené tak, aby boli modulárne podľa požiadavky na škálovateľnosť úložiska (možnosť pridávania kapacity) a súčasne modulárne pre implementáciu dodatočných hardvérových prostriedkov s cieľom zvýšenia výkonu.

Pre server, ktorým spoločnosť už disponuje, je navrhovaná nová aplikácia. V návrhu sa počíta s jeho využitím na archiváciu dokumentov, t. j. ako archívneho servera. Archívny server

je druhou časťou úložiska, kde vzhľadom k počtu operácii (frekvencia prístupov je oproti IoT úložiska veľká), charakteru ukladaných dát (súbory rôznej veľkosti a typu) a požadovanej kapacity (podstatne nižšia oproti IoT dátam) je vhodné zvoliť jednoduchší prístup. Navrhuje sa pole typu RAID 1, čiže jednoduché zrkadlenie dát z troch diskov (celková kapacita 30 TB) a predpokladá sa vyššia zodpovednosť zamestnancov za svoje dáta. Výhodou riešenia je vysoká rýchlosť čítania a zápisu, jednoduchosť a nižšia cena. Nevýhodou je vyššia pravdepodobnosť straty dát.

Za základné jednotky obidvoch diskových polí sú zvolené disky HDD kapacity 10 TB (WD Gold). Výhodou voľby jediného typu disku je zjednodušenie správy a možnosti rýchlej reakcie pri zlyhaní akéhokoľvek disku jeho substitúciou. Systém úložiska sa navyše nekomplikuje o ďalší faktor, ktorý by sa mal zvažovať z dôvodu kompatibility alebo vzájomného vplyvu rôznych diskov pri operáciách s dátami. Zároveň bola zvolená taká kapacita jediného disku, aby bol disk sám o sebe dostatočným úložiskom. Typ disku HDD bol zvolený preto, že je oproti SSD stabilnejším, jeho výkon s využitou kapacitou príliš nekolíše a tiež dosahuje vyšší počet možných zápisov. Nevýhodou tohto riešenia bude nižší výkon pri zápise a čítaní dát.

3.4.2 Analýza nákladov na zvolené riešenie

Náklady na navrhované riešenie je možné rozdeliť do niekoľkých skupín. Sú to náklady investičné na zaobstaranie nových zariadení, náklady na prevádzku zariadení (energie, servis a údržba) a náklady spojené so školením personálu. Najjednoduchšie je stanoviť náklady investičné a ročné energetické náklady na prevádzku. Do analýzy nákladov sa preto berú do úvahy ceny zariadení a cena za spotrebovanú energiu. Jednoduchá analýza nákladov je v Tab. 3.5. Nižšie je uvedený zoznam vybraných zariadení, s ktorými návrh počíta.

Zariadenia:

- Router HPE JG409B
- L3 Switch Catalyst WS-C2960X-24TS-L
- L2 Switch Zyxel GS2220-50HP-EU0101F
- WiFi Router Cisco C897VAGW-LTE-GAEK9
- Vyrovnávač záťaže Cisco ASA 5508-X
- Firewall Zyxel VPN1000-EU0101F
- Kábel Cat 6
- Kábel Cat 7
- NAS Server Synology DS2419+
- HDD WD Gold 10 TB
- UPS Zdroj APC Smart-UPS 2200 VA LCD 230 V

Ceny za energetickú jednotku €/ kWh boli vypočítané na základe tarify platnej pre malé podniky stanovenej za rok 2021 [30].

Tab. 3.5: Analýza investičných a prevádzkových nákladov [22,26,30]

Zariadenie	Jednotková cena	Množstvo	Spotreba energie rok/cena	Nákupná cena
Router HPE JG409B	2 000 €	2 ks	1 052 kWh/ 94 €	4 000 €
L3 Switch Catalyst WS-C2960X-24TS-L	930 €	2 ks	858 kWh/ 72 €	1 860 €
L2 Switch Zyxel GS2220-50HP-EU0101F	990 €	4 ks	1 660 kWh/ 136 €	3 960 €
WiFi Router Cisco C897VAGW-LTE-GAEK9	1 000 €	2 ks	1052 kWh/ 94 €	2 000 €
Vyrovnávač záťaže Cisco ASA 5508-X	1 100 €	2 ks	1052 kWh/ 94 €	2 200 €
Firewall Zyxel VPN1000-EU0101F	1 400 €	2 ks	806 kWh/ 130 €	2 800 €
Kábel Cat 6	0,8 €/m	15 m		12 €
Kábel Cat 7	1 €/m	735 m		735 €
NAS Server Synology DS2419+	1 400 €	2 ks	1 780 kWh/ 145 €	2 800 €
HDD WD Gold 10 TB	280 €	41 ks	3321 kWh/ 280 €	11 480 €
UPS Zdroj APC Smart-UPS 2200 VA LCD 230 V	1 000 €	1 ks		1 000 €
Celkové náklady	**Ročné prevádzkové náklady**		**1 100 €**	
	Cena investície		**33 000 €**	

3.5 Nové procesy zálohovania a obnovenia

Nasadením nového lokálneho úložiska a zmenou spôsobu zálohovania, musia byť taktiež upresnené nové procesy zálohovania a obnovenia dát, ktorými sa budú zamestnanci v daných situáciách riadiť, aby boli procesy plynulé a efektívne.

3.5.1 Plány obnovy pri poruche

Vďaka lepšiemu spôsobu zálohy dát bude ich obnova jednoduchšia, komplexnejšia a efektívnejšia.

Zlyhanie lokálneho úložiska

V prípade zlyhania jedného z diskov, bude disk nahradený a spustí sa obnova dát. Obnova dát na archivačnom serveri bude spustená až na konci dňa a to z dôvodu, že je na serveri aplikovaný RAID 1, takže dáta budú stále dostupné. Záloha NAS serveru bude spustená okamžite, z dôvodu využitia RAID 6. Počas obnovy bude prenos dát medzi cloudom a lokálnym úložiskom pozastavený, až do doby obnovenia zálohy. Cieľom je čo najrýchlejšia správna obnova dát. Komplexnosť obnovy musí byť skontrolovaná aspoň dvoma zamestnancami.

Cloud server

V tomto prípade ide najmä o ľudský faktor, keďže prenos dát je zabezpečený dostatočne rovnako ako ochrana dát na cloude. Ak nastane problém neúmyselnej aktualizácie súboru alebo z nejakých dôvodov bude požadovaný prístup ku predchádzajúcej verzii súboru, postačí si na cloude vybrať staršie verzie súborov, ktoré spolu s aktuálnou verziou zostávajú na cloude uložené. Vymazané dáta zostávajú k dispozícii po dobu, ktorú si spoločnosť určí na základe aktuálnej politiky zálohovania. Pre zamestnanca pred uplynutím tejto doby postačuje súbory obnoviť z archívnych dát cloudu. Obnova bude okamžitá a zaberie minimum času.

Pracovné stanice

Za zálohu pracovných staníc budú zodpovední zamestnanci, vytváranie lokálnej zálohy na pracovnej stanici je povinné, riadené firemnou politikou a spravované systémovým integrátorom. Možnosť obnovenia dát pri poškodení disku na pracovnej stanici, je daná dôsledným dodržiavaním firemnej politiky zálohovania dôležitých dokumentov na iné úložisko. Pri dodržaní dôsledného zálohovania, je možné dôležité dáta pracovných staníc obnovovať z úložísk. Takto je dosiahnutý stav, za ktorého pri poškodení jednej z pracovných staníc, nenastáva problém straty dát a to vďaka ukladaniu všetkých dát na serveri NAS alebo na cloud.

3.5.2 Politika zálohovania

Po realizácii navrhovaného riešenia by boli dáta zabezpečené výrazne lepšie oproti pôvodnému riešeniu. Lokálne servery s aplikovaným RAID 6 a RAID 1 sú z hľadiska zálohovania odolnejšie voči interným aj externým hrozbám. Do siete je nepovolený prístup komplikovanejší a úložisko je lepšie zabezpečené. Individuálne poškodenie disku nespôsobí stratu dát. Dáta sú z krátkodobého hľadiska zálohované na cloude a z dlhodobého hľadiska je využité lokálne úložisko. Na správne využívanie dát a ich zálohovanie je potrebné vzhľadom k novému konceptu definovať nové politiky zálohovania. Z politiky zálohovania by malo byť zrozumiteľné, ako má byť konkrétne úložisko využité, aký typ dát sa môže na dané úložisko ukladať, ako narábať s dátami rôznej priority (kategorizácia) a nakoniec frekvencia zálohovania dát podľa úložiska a kategórie.

Politika zálohovania dát na cloude reflektuje potrebu krátkodobej zálohy a následného nahradenia dátami novými. Na cloude sa predovšetkým zavádza povinná kategorizácia, podľa ktorej budú dáta z cloudu presunuté na určené úložisko, prípadne existuje možnosť dočasného odkladu vymazania dát s nastaveným príznakom (podrobnejšie diskutované v kap. 3.1.1).

Všetky dáta uložené na cloude budú týždenne kontrolované a následne presunuté na lokálne úložisko alebo vymazané.

Lokálne úložisko pre IoT dáta má na dlhodobé uloženie prijímať dáta z cloudu, prípadne priamo od zákazníkov. Spôsob distribúcie jednotlivých IoT tokov do piatich nezávislých uzlov tvorených NAS servermi, nie je v tejto práci presne definovaný. Distribúcia by mala byť optimalizovaná pre rovnomerné naplnenie kapacity uzlov, logické uloženie podľa zdrojov dát alebo podľa metódy ich spracovania a analýzy. Koncept úložiska distribúciu umožňuje, ale presný algoritmus by mal byť vypracovaný na základe dôkladnej znalosti dát dátovými analytikmi. Ostatné dokumenty a súbory určené pre dlhodobú zálohu podľa priority a kategórie budú zálohované na archivačnom serveri. Kontrola obsahu dát IoT úložiska pre posúdenie užitočnosti zálohovaných dát a rozhodnutie o vymazaní sa má vykonávať v ročnej perióde. V prípade archivačného serveru budú dáta overované polročne, aby sa prehodnotila potreba uchovávania daných dát. Dodatočná záloha mimo navrhnutých úložísk je možná pomocou externých HDD, po dôkladnom posúdení dát alebo na osobnú zodpovednosť pri kategórii dát Personal. Obsah externého HDD má byť posudzovaný na dennej báze. Ak sa rozhodne zo zmysluplných dôvodov, je možné niektoré dáta archivovať na externých HDD dlhodobo a kontrolovať ich v dlhšej perióde.

Na lokálnom úložisku budú dáta zálohované inkrementálne, z dôvodu urýchlenia procesu zálohovania. V Tab. 3.6 sú zobrazené kategórie dát, s cieľovou lokalitou pre ich zálohovanie a frekvenciou vytvárania záloh.

Tab. 3.6: Frekvencia a cieľová lokalita zálohovaných dát podľa kategórie

Kategória dát	**Lokalita**	**Frekvencia**
Customers	Cloud	Denne
Finished_projects	Archivačný server	Týždenne
Projects	Cloud	Denne
Data_reports	Cloud	Denne
Management	Archivačný server	Mesačne
Marketing	Archivačný server	Týždenne
Accounting	Archivačný server	Mesačne
Employees	Archivačný server	Ročne
Logistics	Archivačný server	Mesačne
Personal	Externý HDD	Denne
IoT	IoT úložisko	Denne

3.5.3 Zodpovedné osoby

Zálohovanie a správa dát je komplexný problém, ktorého súčasťou spoločnosti nie sú len technické prvky, ale na plynulom fungovaní dátového úložiska a spojených systémov je potrebné jednoznačne zadefinovať zodpovednosť za procesy, ktoré súvisia so zálohovaním a narábaním s dátami. Pozície zodpovedné za jednotlivé procesy sú priradené v Tab. 3.7. V prideľovaní zodpovednosti za dáta, sa postupuje podľa pravidla, že najkompetentnejšími osobami sú priami nadriadení pracovníkov z jednotlivých oddelení. Títo by mali mať o daných dátach najlepší prehľad. V ich kompetencii bude možnosť pridelené dáta, ktoré sú už súčasťou úložiska meniť alebo mazať. Najvyššia autorita pre nakladanie s dátami je riaditeľ IT, ktorý má kompetenciu sám rozhodnúť o manipulácii s akýmikoľvek dátami, ale odporúča sa postup konzultácie so zodpovednou osobou nižšej úrovne. Na neustále sa meniacu situáciu je vhodné zaviesť bezpečnostné audity a školenia, kde ako zodpovedné osoby vystupujú určení pracovníci spoločnosti a externí pracovníci vykonávajúci audit.

Tab. 3.7: Rozdelenie zodpovednosti za jednotlivé procesy spojené s využívaním dát

Proces	Zodpovedná pozícia
Zodpovednosť za IoT dáta	Riaditeľ IT, Dátový analytici
Zodpovednosť za dáta manažmentu a marketingu	Personálny manažér
Zodpovednosť za obchodné dáta	Obchodný zástupca
Zodpovednosť za dáta z účtovníctva	Finančný manažér
Zodpovednosť za dáta logistiky	Manažér logistiky
Zodpovednosť za IT a projektové dáta	Projektový manažér a development administrátor
Servis serverov	Hardvérová podpora
Správa siete	Správca sietí
Politika siete	Správca sietí
Overenie dát a rozhodnutie o vymazaní	Riaditeľ IT
Audit bezpečnosti siete	Správca sietí, externý pracovník
Audit procesu zálohovania	IT podpora ,externý pracovník
Školenie IT bezpečnosti	Správca sietí, externý pracovník

ZÁVER

Návrhom redundantného lokálneho úložiska, do ktorého je možné presúvať dáta zo zavedeného cloudu, pri rešpektovaní zásad bezpečnosti a ochrany dát, bol splnený hlavný cieľ práce. Východisko pre riešenie boli teoretické poznatky a odporúčania popísané v teoretickej časti práce. Komplexné riešenie bolo rozdelené do troch blokov, pretože sa ako optimálne ukázalo zjednodušenie problému na časť týkajúcu sa zmien na cloude, návrhu sieťovej infraštruktúry a vlastného lokálneho úložiska. Na základe navrhovaného riešenia je možné vyjadriť niekoľko nasledujúcich podstatných záverov.

Cloudové úložisko zostáva zachované v doterajšej kapacite, zmeny spočívajú v zavedení kategorizácie dát, ktorá umožňuje dáta efektívne presúvať a zálohovať na lokálne úložisko. Výhody cloudu sú využité pre krátkodobú prácu a projekty. Využitá je výpočtová kapacita cloudu a aplikácie pre prácu s dátami. Okrem krátkodobej práce zostáva cloud dlhodobým úložiskom pre mailovú komunikáciu spoločnosti.

Sieťová infraštruktúra je navrhnutá redundantne, s pripojením k dvom nezávislým poskytovateľom. Štruktúra siete je hierarchická a organizovaná od úrovne chrbticovej siete až k menším jednotkám, ktoré tvoria jednotlivé oddelenia a lokálne úložisko. Na organizáciu siete je využitý protokol OSPF a pre menšie celky zavedené VLANy. Požiadavka na výkonnosť je splnená výberom hardvérových prvkov, logickým usporiadaním štruktúry siete a vhodným dimenzovaním kritických miest. Bezpečnosť je vyriešená zavedením hardvérových zariadení do siete a vytvorením logicky a fyzicky chránených celkov. Zvýšená ochrana dátového úložiska spočíva v zriadení DMZ.

Lokálne dátové úložisko je rozdelené na dve časti. Časť pre zálohu IoT dát a časť pre archiváciu ostatných dokumentov a súborov tvorenú archivačným serverom. IoT úložisko je dimenzované na vysokú kapacitu až 200 TB, so zavedením ochrany metódou RAID 6. Prípadná strata dvoch diskov jedného uzlu úložiska by nemala mať fatálne následky. Uzly IoT úložiska sú vytvorené NAS servermi a v každom uzle je pre dodatočnú ochranu zaradený pohotovostný spare disk. Archivačný server je dimenzovaný na nižšiu kapacitu 30 TB, ktorá je zálohovaná jednoduchým zrkadlením metódou RAID 1.

ZOZNAM POUŽITEJ LITERATÚRY

[1] B. Posey, What is backup?, (2016). http://searchdatabackup.techtarget.com/definition/backup (cit 31. marec 2021).

[2] J. Yu, What is data archiving? - Definition from WhatIs.com, Https://Searchdatabackup.Techtarget.Com/Definition/Data-Archiving. (2015). https://searchdatabackup.techtarget.com/definition/data-archiving (cit 31. marec 2021).

[3] Consoltech, Data Loss: Causes, Effects & Prevention Methods | Consolidated Technologies, Inc., 2021. (n.d.). https://consoltech.com/blog/10-common-causes-of-data-loss/ (cit 30. marec 2021).

[4] P. Crocetti, What is data compression? - Definition from WhatIs.com, (2017). https://searchstorage.techtarget.com/definition/compression (cit 31. marec 2021).

[5] Data duplication, 2017. (n.d.). https://www.handybackup.net/backup_terms/data_duplication.shtml (cit 01. apríl 2021).

[6] H. Spots, F. What, W. Fidelity, What is Wi-Fi and how does it work ? What is Wi-Fi and how does it work ?, (2014) 5–6.

[7] E. Sullivan, C. Poelker, S. Peterson, Comparing RAID levels: 0, 1, 5, 6, 10 and 50 explained, (2020). https://searchstorage.techtarget.com/answer/RAID-types-and-benefits-explained (cit 29. marec 2021).

[8] E. Sullivan, What is RAID 10 (RAID 1+0)?, Tech Target. (2017). https://searchstorage.techtarget.com/definition/RAID-10-redundant-array-of-independent-disks (cit 30. marec 2021).

[9] Computer Hope, What is a Hard Drive?, Comput. Hope. (2018) 1. https://www.computerhope.com/jargon/h/harddriv.htm (cit 30. marec 2021).

[10] Computer Hope, What is SSD (Solid-State Drive)?, (2018). https://www.computerhope.com/jargon/s/ssd.htm (cit 30. marec 2021).

[11] T. Hort, Technologie a zajímavosti z oblasti SSD disků, (2011). https://pctuning.tyden.cz/hardware/disky-cd-dvd-br/22588-technologie-a-zajimavosti-z-oblasti-ssd-disku (cit 30. marec 2021).

[12] A. Miller, What is direct-attached storage (DAS)? - Definition from WhatIs.com, (2018). https://searchstorage.techtarget.com/definition/direct-attached-storage (cit 03. apríl 2021).

[13] Techtarget, What is Network Attached Storage? - Definition from WhatIs.com, (2019). https://searchstorage.techtarget.com/definition/network-attached-storage (cit 06. apríl 2021).

[14] Stephen J. Bigelow, What Is a Storage Area Network? SAN Explained, (n.d.). https://searchstorage.techtarget.com/definition/storage-area-network-SAN (cit 07. apríl 2021).

[15] Stephen J. Bigelow, What is hybrid cloud? - Definition from WhatIs.com, (2015). http://searchcloudcomputing.techtarget.com/definition/hybrid-cloud (cit 19. apríl 2021).

[16] S. Neenan, What is public cloud? - Definition from WhatIs.com, TechTarget. (2009).

http://searchcloudcomputing.techtarget.com/definition/public-cloud (cit 24. apríl 2021).

[17] A. Miller, What is private cloud storage (internal cloud storage)? - Definition from WhatIs.com, SearchStorage. (2019). https://searchstorage.techtarget.com/definition/private-cloud-storage-internal-cloud-storage (cit 24. apríl 2021).

[18] T. Contributor, What is data virtualization? - Definition from WhatIs.com, 2019. (n.d.). https://searchdatamanagement.techtarget.com/definition/data-virtualization (cit 29. apríl 2021).

[19] K. Huang, Z. Li, The campus cloud platform setup based on virtualization technology, Procedia Comput. Sci. 183 (2021) 73–78. https://doi.org/10.1016/j.procs.2021.02.032.

[20] C. Wesley, What is cloud computing? Everything you need to know about the cloud, explained, SearchStorage. (2018). https://searchcloudcomputing.techtarget.com/definition/cloud-computing (cit 24. apríl 2021).

[21] H. Jiang, F. Shen, S. Chen, K.C. Li, Y.S. Jeong, A secure and scalable storage system for aggregate data in IoT, Futur. Gener. Comput. Syst. 49 (2015) 133–141. https://doi.org/10.1016/j.future.2014.11.009.

[22] Senetic, (2019). https://www.senetic.sk/ (cit 04. máj 2021).

[23] Cisco, DMZ Options for RV160/RV260 Routers - Cisco, (2018). https://www.cisco.com/c/en/us/support/docs/smb/routers/cisco-rv-series-small-business-routers/smb5875-dmz-options-for-rv160-rv260-routers.html (cit 11. máj 2021).

[24] B. Lutkevich, What is a DMZ and How Does it Work?, Https://Searchsecurity.Techtarget.Com/. (2019). https://searchsecurity.techtarget.com/definition/DMZ (cit 12. máj 2021).

[25] J.F. Kurose, K.W. Ross, Počítačové sítě, 1., Computer Press, a.s., Brno, 2014.

[26] Pevné disky | Hard disky | Alza.sk, (n.d.). https://www.alza.sk/pevne-disky/18842851.htm (cit 04. máj 2021).

[27] M. Gilroy, J. Irvine, R. Atkinson, RAID 6 hardware acceleration, Trans. Embed. Comput. Syst. 10 (2011). https://doi.org/10.1145/2043662.2043667.

[28] Synology, RAID Calculator | Synology Inc., Synology.Com. (n.d.). https://www.synology.com/en-uk/support/RAID_calculator?hdds=8 TB%7C8 TB%7C8 TB%7C8 TB%7C8 TB%7C8 TB%7C8 TB%7C8 TB (cit 12. máj 2021).

[29] Microsemi, Choosing the Right RAID Configurations | Microsemi, (n.d.). https://www.microsemi.com/product-directory/raid-controllers/4047-raid-levels#2 (cit 13. máj 2021).

[30] Ceny elektriny - Podnikatelia | VSE a.s., (2021). https://www.vse.sk/web/sk/firmy-a-organizacie/elektrina/ceny-elektriny (cit 13. máj 2021).

ZOZNAM SKRATIEK A SYMBOLOV

API	Application Program Interface
ATA	AT Attachment
BGP	Border Gateway Protocol
CEO	Chief Executive Officer
CPU	Central Processing Unit
DAS	Direct-Attached Storage
DLP	Data Loss Prevention
DMZ	Demilitarizovaná zóna
DNS	Domain Name System
DoS	Denial of Service
ESP	Encapsulation Security Payload
HBA	Host Bus Adapter
HDD	Hard Disk Drive
HR	Human Resources
IaaS	Infraštruktúra ako Služba
IK	Internet Keys Exchange
IPSec	IP Security
MLC	Multi-Level Cell
NAS	Network-Attached Storage
NFSv3	Network File System verzia 3.
OS	Operačný systém
OSPF	Open Shortest Path First
PaaS	Platforma ako Služba
RAID	Redundant Array of Independent Disks
SaaS	Softvér ako Služba
SAML 2.0	Security Assertion Markup Language verzia 2.0
SAN	Direct-Attached Storage
SATA	Serial AT Atachment
SCSI	Small Computer System Interface
SLC	Single-Level Cell
SSD	Solid State Drive
SSO	Single Sign-on
UPS	Uninterrutible Power Supply
VPN	Virtual Private Network

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK